HUNGARY`S ALTERNATIVE TO COUNTER HYBRID WARFARE – SMALL STATE`S WEAPONIZED CITIZENRY

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

ADRIAN FEHER, MAJOR, HUNGARIAN ARMY
Bachelor of Military Leadership, Miklós Zrínyi National Defence University, Szentendre, 2001

Fort Leavenworth, Kansas
2017

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
9-06-2017	Master's Thesis	AUG 2016 – JUNE 2017

4. TITLE AND SUBTITLE

Hungary`s Alternative to Counter Hybrid Warfare – Small State`s Weaponized Citizenry

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Adrian Feher

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The dawn of the 21st century introduced a more complex and sophisticated threat than the NATO (North Atlantic Treaty Organization) has experienced since the Cold War. This hybrid threat is only partially military in nature; it applies to informational, economic, and diplomatic instruments to weaken nation-states and even NATO itself. Moreover, hybrid warfare targets the population and exploits its vulnerability against contradictory propaganda. Hungary has to align with NATO counter hybrid exertion; hence, it has to establish her own national resilience capability. Hungary has already expressed her commitment to augment reserve forces capability. Reserve forces intend to extend the capacity of the active segment and to strengthen relations between the defense sector and civil society. This thesis seeks to determine if there is more potential with the involvement of civilian population segments in the nation`s defense. While the conventional type, volunteer reserve force can offer traditional defense capability and encompass only a segment of the population, non-traditional means can extend military capacity and the citizenry`s involvement to foster resilience. The thesis examines those synergetic effects between military and information instruments of national power, which can extend the resilience capability, and hence generate further options for decision-makers.

15. SUBJECT TERMS
Hybrid Warfare, Unconventional warfare, Resilience, Resistance, Civil preparedness, NATO, SOF

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	160	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Adrian Feher

Thesis Title: Hungary`s Alternative to Counter Hybrid Warfare – Small State`s Weaponized Citizenry

Approved by:

_____, Thesis Committee Chair
David T. Culkin, Ph.D.

_____, Member
Brigadier General Imre Porkolab, Ph.D.

_____, Member
Lieutenant Colonel Adam S. Talkington, M.S.

Accepted this 9th day of June 2017 by:

_____, Director, Graduate Degree Programs
Prisco R. Hernández, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

HUNGARY`S ALTERNATIVE TO COUNTER HYBRID WARFARE – SMALL STATE`S WEAPONIZED CITIZENRY by Major Adrian Feher, 160 pages

The dawn of the 21st century introduced a more complex and sophisticated threat than the NATO (North Atlantic Treaty Organization) has experienced since the Cold War. This hybrid threat is only partially military in nature; it applies to informational, economic, and diplomatic instruments to weaken nation-states and even NATO itself. Moreover, hybrid warfare targets the population and exploits its vulnerability against contradictory propaganda. Hungary has to align with NATO counter hybrid exertion; hence, it has to establish her own national resilience capability. Hungary has already expressed her commitment to augment reserve forces capability. Reserve forces intend to extend the capacity of the active segment and to strengthen relations between the defense sector and civil society. This thesis seeks to determine if there is more potential with the involvement of civilian population segments in the nation`s defense. While the conventional type, volunteer reserve force can offer traditional defense capability and encompass only a segment of the population, non-traditional means can extend military capacity and the citizenry`s involvement to foster resilience. The thesis examines those synergetic effects between military and information instruments of national power, which can extend the resilience capability, and hence generate further options for decision-makers.

ACKNOWLEDGMENTS

I deeply appreciate my family, my wife Krisztina also my kids Zsombor and Csenge, for supporting me during research and writing, as well as for their understanding that I spent less time with them than they desired. Particular thanks are due to my committee, Dr. David T. Culkin, BG Imre Porkolab, and LTC Adam S. Talkington, who keep me on the right track through their demand for rigor. I want to thank to Errett Schmid who spent countless hours to correct my thesis grammatically and became my first audience with her husband, Jack. Finally, I have to recognize my parents who taught me to be persistent.

TABLE OF CONTENTS

Page

ACRONYMS

CAO	Civil Affairs Operations
DIME	Diplomacy, Information, Military and Economy (The DIME framework)
EU	European Union
HDF	Hungarian Defense Forces
IW	Irregular Warfare
JISR	Joint Intelligence Surveillance and Reconnaissance
MISO	Military Intelligence Support Operations
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NRF	NATO Response Forces
PMESII-PT	Political, Military, Economic, Social, Information, Infrastructure, Physical environment and Time
SF	Special Forces
SFA	Strategic Foresight Analysis
SO	Special Operations
SOF	Special Operation Forces
TDF	Territorial Defense Forces
UN	United Nations
UW	Unconventional Warfare
VJTF	Very High Readiness Joint Task Force

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

> When a whole nation renders armed resistance, the question then is no longer, "Of what value is this to the people," but "what is its potential value, what are the conditions that it requires, and how is it to be utilized."
>
> — Carl von Clausewitz, *On War*

A small country, such as Hungary, is more vulnerable against hybrid threat that a great power can utilize to attack a weaker state. The aggressor has supremacy in Diplomacy, Informational, Military, and Economic (DIME) instruments of national power, and it intends to influence these instruments of Hungary simultaneously in order to achieve advantage over the country. The nation must understand the threat against its sovereignty, which is hybrid in nature and requires more than Military approach to counter it. North Atlantic Treaty Organization (NATO), from the perspective of the entire alliance, and other small states are already looking for solutions to neutralize hybrid threats. Hungary has to examine these endeavors and select or combine those that are relevant and effective in her unique security and social environment. The solution cannot be simple, but complex, comprehensive, and synchronized as the hybridized threat itself. Moreover, the involvement of citizenry is not avoidable, because only through and with the people could a small state possess an adequate and sustainable deterrence or defeat capability against a superior adversary.

The first chapter provides a comprehensive picture of Hungary`s defense challenges in the beginning of the 21st century. The primary challenge is correlation with hybrid warfare, which overshadows the entire Western society. In order to illustrate the effect of hybrid warfare, the first chapter will examine the contemporary defense posture

of Hungary, the changes in the present international security environment, and the influence of these changes on NATO, which are affecting Hungarian defense policy. This context analysis provides a foundation for the study`s problem statement and the research question, which will anticipate a non-traditional alternative to overcome or mitigate the effect of hybrid challenges. Assumptions, definitions, limitations, and the significance of this paper will clarify the subject, and narrow its focus to a military-centric approach that can involve citizens in the nation`s defense.

Background

After the disintegration of the Warsaw Pact ending the bipolar world, the direct threat to Hungary as a buffer zone between two super-powers was meaningfully reduced. Hungary, like other nations in the region, significantly decreased and restructured its military capacity. The elimination of the Cold War threat, and NATO membership in 1999 led to the derogation of the defense budget, the suspension of mandatory conscription in 2004, and the establishment of a volunteer active duty force. NATO membership allowed Hungary to become a part of the most powerful political and military alliance and provided large-scale security. The membership also embodied several obligations from the state to support Alliance objectives and endeavors. For more than 15 years "Hungary does not consider any country as its enemy"[1] hence the Hungarian Defense Forces (HDF) were focused mainly on deploying to United Nations

[1] Hungarian Ministry of Defence, "Hungary`s National Defence Strategy," Website of the Hungarian Government, 2012, accessed March 28, 2017, http://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf#!DocumentBrowse, 5.

and NATO missions, disaster relief operations,[2] and recently were heavily involved in the counter migration mission.[3] Simultaneously regular formations and Special Operation Forces have been integrating with NATO standards, although financial shortfalls and an increasing workload have slowed these efforts. While the HDF supports NATO`s level of ambition, the security environment in the region has been abruptly and significantly changed by Russian aggression against Ukraine, and demands a new approach from the alliance, as well as from Hungary.[4]

Although Hungary has not directly suffered a Russian attack so far, the challenge that Russia introduced in the Ukraine blurred the boundaries of current military doctrine and necessitated a different approach to win a contemporary conflict. 21st century warfare has different terms: new generation, ambiguous, hybrid, nonlinear, unrestricted.[5] Each term expresses the disappearance of the visible border between war and peace, the danger of divisive propaganda, the application of every single domain, the involvement of non-state actors, the shrinkage of early warning and the threat against the nation`s

---

[2] Peter Marton, and Peter Wagner, "The Impact of Hungary`s NATO Membership. Intra-Allience Adaptation between Soft Constrains and Soft Subversion," in *Newcomers No More? Contemporary NATO and the Future of the Enlargement from the Perspective of 'Post-Cold War' Memebers*, ed. Robert Czulda and Marek Madej (Warsaw, Prague, Brussels: International Relation Research Institute in Warsaw, NATO Information Center in Prague, 2015), 138-140.

[3] Hungarian Ministry of Defence, "Hungarian Defence Forces," accessed January 17, 2017, http://www.honvedelem.hu/files/9/5294/imazs-angol.pdf.

[4] Marton and Wagner, 148-151.

[5] Victor R. Morris, "Grading Gerasimov-Evaluating Russian Nonlinear War through Modern Chinese Doctrine," *Small Wars Journal*, September 17, 2015, accessed January 2, 2017, http://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine.

entire Diplomatic, Information, Military and Economic power structure. The DIME framework expresses how a nation can influence the international system to achieve national strategic objectives,[6] hence its ability to project power. Hybrid warfare is not primarily military in nature, but by Diplomatic, Information and Economic instruments is able to destabilize a nation state or even threaten its sovereignty.[7] Furthermore, the threat from the east is not exclusively against independent states, but intends to subvert NATO, and other international organizations like the European Union.

NATO has already reflected on the new security challenges and during the NATO Summit meeting in Warsaw, 8-9 July 2016, resulted in Alliance leaders acknowledging the need to enhance capacities to confront emerging contemporary threats posed by hybrid warfare. The NATO Summit Resilience Commitment communique, and the U.S. President`s European Reassurance Initiative also emphasize the importance of the protection of new NATO members' critical defense vulnerability. The NATO Summit highlighted the close connection between Article 3-the individual responsibility for self-defense, and resilience-the resisting and recovering capability. In other words, members have to develop their individual capability to resist against an armed attack, and simultaneously improve the ability of the society to resist and recover easily and quickly from military and non-military shocks.[8]

---

[6] Joint Chief of Staff, Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: Joint Chief of Staff, 2013), I-11.

[7] Andras Racz, "Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist" (FIIA Report, Helsinki, Finland: The Finnish Institute of International Affairs, 2015), 51.

[8] NATO, "NATO Summit Guide Warsaw 8-9 July 2016," NATO Public Diplomacy Division, accessed January 11, 2017, http://www.nato.int/nato_static

In accordance with the Warsaw NATO Summit, Hungary also communicated its commitment to increase defense expenses and to invest in reserve forces. Minister of Defense, Dr. Istvan Simicsko, said "Relations must be strengthened between the Hungarian Defense Forces and society."[9] The Minister also announced a plan for the establishment of a territorial based reserve force, and about the young population`s involvement in patriotic education.[10] This thesis examines if there are other feasible ways for Hungary to assist increasing the nation`s resilience.

Significance of the Problem

Contemporary security challenges originating from hybrid warfare demand new approaches from the Hungarian Defense Forces, and a modification of the National Military Strategy. Potential adversaries will seek for vulnerabilities in each instrument of national power and exploit them to degrade Hungary`s capability to resist. Before open armed conflict, unless the attack crosses NATO Article 5 threshold, the alliance's collective defense will not take effect; thus, Hungary has to prepare to defend its own national interests.[11] As a small state, Hungary cannot depend solely on regular military

_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf, 131.

[9] Hungarian Ministry of Defence, "Relations Must Be Strengthened between the Hungarian Defense Forces and Society," Website of the Hungarian Government, November 25, 2016, accessed January 17, 2017, http://www.kormany.hu/en/ministry-of-defence/news/relations-must-be-strengthened-between-the-hungarian-defence-forces-and-society.

[10] Ibid.

[11] NATO, "NATO Summit Guide Warsaw," 131.

instruments, but has to involve the whole might of its national defense capabilities, including the population, in an integrated manner to complement the regular armed forces and successfully counter non-traditional challenges.

The HDF has to maintain a strong deterrence posture, and if deterrence fails, has to prepare for initiating countermeasures against a multi-domain, ambiguous threat. Therefore, the HDF needs a paradigm change, to ensure capability augmentation (across the whole spectrum), agile decision-making, and reduced reaction time. The desired national defense capability has to have similar characteristics with the hybrid one: maintains control over DIME structure, maximizes unity of effort, and possesses adequate military strength, supportive and involved population, cyber defense capacity, effective intelligence and counterintelligence.[12] However, Hungary has to achieve this end state democratically in order to preserve her position in NATO and Europe, and to maintain long-term civilian support.

The civilian population has a significant amount of capacity to complement the military; therefore, the involvement of the civilian sector in building resilience is indispensable.[13] However, at present, popular opinion on this issue is divided at best, thus we need to raise awareness of recognizing the generally invisible threat of hybrid warfare.[14] In hybrid warfare, the population is the primary target of the aggressor`s

---

[12] Aapo Cederberg and Pasi Eronen, "How Can Societies Be Defended Against Hybrid Threats," Fortuna`s corner, November 6, 2015, accessed November 12, 2016, http://fortunascorner.com/2015/11/06/how-can-societies-be-defended-against-hybrid-threats/, 8.

[13] Ibid.

[14] Marton and Wagner, 146.

propaganda.[15] Ambiguous propaganda easily confuses people`s views through the effective use of the Information instrument of the nation`s power, hence significantly reducing the capability to respond to hostile intent.[16] The Information power is vital for the nation to prepare the citizenry for negative influence of opponents, to regain interaction between the state and people, and to terminate the citizens` false sense of security.

Purpose

Hungary has to adjust her national defense strategy to meet the demands of the hybrid threat, and to focus more on developing capabilities to meet Article 3 criteria in order to support the new NATO resilience posture. The new defense strategy must address issues like protecting elements of the state`s DIME structure from asymmetric threats, and has to cover all domains–including cyber. Former studies on countering hybrid warfare have identified these requirements as well as underscored the key importance of the involvement of civilian society. However, scholars have not examined how Hungary could apply a practical way to defend the nation`s sovereignty through the participation of a large segment of the population in the resilience.

The purpose of this study is to generate options for the HDF decision makers regarding the Military and Informational instruments of national power in order to strengthen Hungary's resilience against hybrid warfare.

---

[15] Racz, 58-59.

[16] Patrick Tucker, "The US Is Losing at Influence Warfare. Here's Why," *Denfense One,* December 5, 2016, accessed February 12, 2017, http://www.defense one.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/.

Problem Statement

The defense sector has to find an applicable solution to reach out, involve, and influence the civilian population in order to increase Hungary`s resilience, the nation`s ability to withstand strategic shocks. Hybrid warfare endangers the civilian sector in order to decrease the legitimacy of the government by aggravating the gap between the state and the citizens. Hungary has to increase her resilience capability against hybrid threats with and through the participation of the citizenry. Contemporary developments in the Information instrument of national power enable unconventional Military ones to extend alternatives beyond the limitations of conventional methods facilitating a better resilience ability for Hungary.

Research Question

In order to identify the most suitable solution to prepare the HDF for hybrid challenges, the study has to answer specific questions. The primary question is: how can interaction between Military and Information instruments of national power facilitate Hungary`s resilience capacity, in order to deter adversaries, and maintain the nation`s sovereignty? Secondary questions will facilitate answering the primary question.

What are the hybrid challenges for which Hungary has to prepare? This question will examine potential threats against Hungary that have emerged in the hybrid environment.

How can Hungary involve its citizenry in order to realize feasible resilience capability? This question is required to survey those areas in defence strategy, where citizens` participation is possible and necessary.

Assumptions

Hybrid warfare, with its highly integrated design, will remain the determinative type of waging war in the foreseeable future. The characteristics of hybrid warfare will change in time and space in order to adapt to the environment, thereby becoming more complex and more sophisticated. Hungary will face conflicts in the gray zone[17], the threats will arise without notice, involve all domains, and various types of stakeholders. Hungary, as a member of NATO, has to align its efforts to establish a common resilience capability against hybrid challenges.

The NATO resilience exertion against contemporary hybrid threat concentrates on states bordering with Russia. Baltic States are the most vulnerable countries sharing similar features with Hungary such as limited maneuver space, limited spending on military, and the strong intent to protect national sovereignty. Their attempt to extend national defense capability by seeking not only regular solutions is an important example for Hungary.

The significance of the cyber domain will further increase, and become the most vital instrument to influence the population, in order to weaken the states` potency. Cyber domain can affect all instruments of DIME, and will grow in the future. Adversaries will take advantage of weakened and fragile states to exercise control over a government or even enable military aggression against the state.

The adversary country or alliance, which is able to challenge members of the NATO, will have significant capability regarding conventional and unconventional forces, cyber warfare and sophisticated information operation capability, and nuclear

[17] "Gray zone" term will be defined on page 16.

deterrence ability. Therefore, the adversary must be a great power, with Diplomatic, Informational, Military, and Economic superiority and strong government, which can wage hybrid war against a small state.

Definition of Terms

Diplomacy, Informational, Military and Economy framework (DIME)

To describe a state`s national power, therefore the state`s ability to achieve the nation`s strategic objective,[18] this study will use the DIME framework. Diplomacy, Informational, Military and Economy instruments are the instruments of national power.

Diplomacy: Joint Publication 1 describes the Diplomatic instrument from the U.S. perspective: "Diplomacy is the principal instrument for engaging with other states and foreign groups to advance . . . values, interests, and objectives, and to solicit foreign support for . . . military operations. Diplomacy is a principal means of organizing coalitions and alliances, which may include states and non-state entities, as partners, allies, surrogates, and/or proxies."[19] Hungary also considers these objectives, but on a smaller scale. NATO membership plays an important role in Hungarian diplomacy, as a primary tool for a small state to preserve its sovereignty. Obligations to the Alliance, such as participating in its three core tasks: collective defense, crisis management and cooperative security,[20] demand significant efforts from each member country. The

[18] Joint Chief of Staff, JP 1, I-11.

[19] Ibid., I-12.

[20] NATO, "NATO Summit Guide Warsaw," 1.

Hungarian government's commitment to increasing military spending and reaching NATO recommendations represents assurance that Hungary wants to become a stronger Ally of NATO.[21]

Information: This instrument synthesizes focused efforts to influence key audiences–domestic, foreign, state or non-state actors – to create, strengthen, or preserve conditions favorable for the advancement of national interests, policies, defense and military objectives.[22] Different actors collect, analyze, apply and disseminate information in order to observe, orient, decide and act upon the result. The information affects the decision making of individuals, organizations and leaders, therefore can influence their deeds.[23] An aggressor would apply the Information instrument to increase the legitimacy of the supported central power, thus discrediting the hostile government, and to gain influence over the relevant population.[24]

In case of hostility against Hungary, the state has to protect the legitimacy of the government, as well as its citizenry on the information domain. Hungary operates in a dynamic age of interconnected global networks and evolving social media platforms, where adversaries can use information to undermine the state and its allies` interest.

---

[21] Hungarian Ministry of Defence, "Relations Must Be Strengthened between the Hungarian Defense Forces and Society."

[22] Joint Chief of Staff, JP 1, I-12.

[23] Headquarters, Department of the Army, Field Manual (FM) 3-05.130, *Army Special Operations Forces Unconventional Warfare* (Washington, DC: Headquarters, Department of the Army, 2008), B-1.

[24] Joint Chiefs of Staff, Joint Publication (JP) 3-05, *Special Operations* (Washington, DC: Joint Chiefs of Staff, 2011), II-1.

Because of the recent elementary changes in the region, the Russian aggression against Ukraine, and the growing migration, Hungary became a battleground of informational warfare.[25]

Military: A nation state "employs the military instrument of national power at home and abroad in support of its national security goals", and to "fight and win the Nation's wars." The military instrument "is coercive in nature, to include the integral aspect of military capability that opposes external coercion."[26]

In the Ukraine-Russian conflict, the military superiority was a key prerequisite for the success of the aggressor, therefore the nation`s military capability remained relevant in hybrid environment.[27] NATO also underlined the significance of Military instrument by reassuring the collective defense endeavor and increasing the Alliance response capability against the traditional military instrument of the hybrid threat.[28]

Hungary has to possess an adequate military capability in order to protect its sovereignty and integrity against adversaries, as well as enable NATO`s collective defense endeavor.[29] This military capability must be ready for the challenges of the current security environment, hence for the hybrid threat as well.

---

[25] Janos T. Barabas, *Information Warfare in Hungary*, (Policy Brief, Budapest: Institute for Foreign Affairs and Trade, 2017), 3.

[26] Joint Chief of Staff, JP 1, I-13.

[27] Racz, 75.

[28] NATO, "NATO Summit Guide Warsaw 2016," 82.

[29] Hungarian Ministry of Defence, "Hungary`s National Defence Strategy," 3-5.

Economy: "A strong . . . economy with free access to global markets and resources is a fundamental engine of the general welfare, the enabler of a strong national defense."[30] As a small country, Hungary does not possess the power to affect the global economy, but international relations are crucial for it to reduce vulnerability and dependence on foreign impact. The Economic instrument possesses most of the limitations for the defense sector, because it provides the means to achieve the ends, defined by diplomacy. The Hungarian Prime Minister, Viktor Orban, expressed that the recent economic improvements enabled more spending on military matters,[31] therefore increasing the capability of armed forces to meet current security challenges.

Small State

The most suitable method to determine the position of Hungary, hence the country`s role in the region, is through the categorization of nation states. There are several different definitions of small states, which examine different aspects of countries. The author will use Hans Morgenthau`s simple approach, which focuses on a state`s will over another one: "A Great Power is a state which is able to have its will against a small state which in turn is not able to have its will against a Great Power."[32]

According to this definition, the economic power, the external resource dependence, the political influence, the dependence on alliances with great powers and

[30] Joint Chief of Staff, JP 1, I-13

[31] Viktor Orban, The Prime Minister of Hungary, Inteview with Viktor Orban, Interview by Katolikus Radio, October 29, 2016.

[32] Hans Morgenthau, *Politics among Nations: the Struggle for Power and Peace* (New York: McGraw-Hill, 1993), 33.

the military strength of Hungary is not comparable to great powers in the region, such as Germany, France, Great Britain, Spain, Italy, and Russia. Therefore, Hungary, as a small state, has to act in accordance with her status.

Hybrid Warfare

This study will use the term "hybrid warfare" to express the character of the Ukraine-Russian conflict. Contemporary scholars utilize different, but not uniformly defined notions, such as new generation, ambiguous, nonlinear, unrestricted, irregular, unconventional and asymmetric.[33] Different regions, countries and scholars use these definitions in dissimilar ways, hence to avoid misunderstanding, this paper will apply the "hybrid warfare" term, currently preferred by NATO.

Following the annexation of Crimea by Russia, military scholars and journalists realized that this type of waging war is somehow different from others in history. They tried to describe this new phenomena, hence reviewed former conflicts to identify similarities, or categorized it with a new term. Finally the NATO`s Wales Summit applied this notion in conjunction with the Ukraine conflict, which has become generally accepted in the Alliance. The NATO Wales Summit declaration defined the hybrid threats, "where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design."[34] Although other hybrid warfare

[33] Morris.

[34] NATO, "Wales Summit Declaration," September 5, 2014, accessed January 30, 2017, http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

definitions specify its means in detail, the declaration highlights hybrid warfare`s integrated design feature.

Racz argued that the only difference between hybrid war and former warfare is the command relationship between Military and other stakeholders. “The only really new element was the skillful and effective coordination of the diplomatic, economic, military, and information instruments used during the operation, all in the framework of a single, well-functioning command structure.”[35] In other words, Russia was able to establish unity of command over different agencies and governmental organizations. In a real democratic state, the unity of effort is the maximum realizable connection among governmental stakeholders,[36] but an autocratic country can achieve stronger command and control relationship.

In contrast, Captain Robert A. Newson`s definition is detailed in instruments, but did not emphasize hybrid warfare`s unique command structure:

> [Hybrid warfare is] . . . a combination of conventional, irregular, and asymmetric means, including the persistent manipulation of political and ideological conflict, and can include the combination of special operations and conventional military forces; intelligence agents; political provocateurs; media representatives; economic intimidation; cyber-attacks; and proxies and surrogates, para-militaries, terrorist, and criminal elements.[37]

Hybrid warfare integrates every possible type of warfare, military and paramilitary formations, state and non-state actors and civilian population to achieve

---

[35] Racz, 51.

[36] Joint Chief of Staff, JP 1, GL-13.

[37] Robert A. Newson, “Why US Needs Strategy to Counter Hybrid Warfare,” *Defense One*, October 23, 2014, accessed January 14, 2017, http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybridwarfare/97259/.

effect on all fields of national power. The novelty of hybrid warfare is the conscious integration of control over ways to achieve a synergic effect. The other advantage is its aggressive offensive nature that hinders adversaries from defending their different vulnerabilities simultaneously.

White, Grey, and Black Zones of Conflicts

While regular and hybrid notions express the differences about how to wage war, the white-gray-black zones of conflict distinguish security environments. The threshold between these zones is tough to define and apply, due to their blurring boundaries. The following definition describes the grey zone`s left and right limits.

"Gray Zone activities are an adversary's purposeful use of single or multiple elements of power to achieve security objectives by way of activities that cloud attribution, and exceed the threshold of ordinary competition, yet apparently fall below the level of large-scale threats to U.S. or allied security interests."[38] The application of this definition is still equivocal. The lack of clarity is the reason for adversaries to operate in this environment, however. Aggressors that challenge NATO in the gray zone must be sure about the threshold of Article 5`s collective defense limit, in order to avoid open armed conflict. The gray zone is the preferable environment for hybrid warfare to utilize its advantages most effectively, and in full spectrum scale.

Until an adversary operates in the gray zone against Hungary, the nation has to solve challenges without the robust support of the Alliance. Under the Article 5

[38] Belinda Bragg, "Specifying and Systematizing How We Think about the Gray Zone," NSI Team, July 27, 2016, accessed January 5, 2017, http://nsiteam.com/social/wp-content/uploads/2016/12/CP-1-Definition-of-Gray-06-27-2016-Final.pdf, 7.

threshold, NATO does not have the authority to support Hungary with the same assets than in collective defense.

Resilience

The Alliance underlined the importance of resistance during the NATO Summit in Warsaw 2016, and expressed "Each NATO member country needs to have the resilience to withstand shocks like natural disasters, failure of critical infrastructure and military attacks." NATO defines resistance as "a society's ability to resist and recover easily and quickly from these shocks, combining civilian, economic, commercial and military factors. In sum, resilience is the combination of civil preparedness and military capacity."[39] Moreover, in the NATO interpretation, there is a strong connection between resilience and Article 3, which covers member`s individual commitment to "develop and maintain capacity to resist armed attack."[40]

Civil preparedness means that "basic government functions can continue during emergencies or disasters in peacetime or in periods of crisis. It also means that the civilian sector in Allied nations would be ready to provide support to a NATO military operation."[41] Since the termination of the Cold War, countries have privatized their key infrastructures; therefore, the state does not possess direct control over these crucial assets.[42] Hungary also has to involve the civil sector to exercise control over these critical

[39] NATO, "NATO Summit Guide Warsaw 2016," 131.

[40] Ibid.

[41] Ibid., 134.

[42] Ibid., 135.

capabilities to enable NATO military operations inside the country.[43] However not just access is important to these capacities, but the state has to secure that access, which is another potential area for civil involvement in resilience.

The other segment of resilience is the military capacity. This capacity includes mainly regular active service forces, but U.S. Special Operations Command Europe sponsored and led Resistance Seminar Series pinpointing the application of irregular type forces, based on resistance.[44] The resistance can involve a large mass of citizens; to augment the capability of regular forces, hence support the Alliance`s endeavor.

Regular, Irregular and Unconventional Warfare

There are two significantly different methods for a nation to build up its military defense strategy. The first extreme is regular warfare, utilizing conventional forces, with the ability to conduct force of force operations. Regular, traditional and conventional warfare are essentially synonym terms.[45] These terms express a form of warfare between states, employing direct military confrontations to defeat enemy forces, seize or retain territory in order to force a change in an adversary's government or policies. It generally assumes that the indigenous populations within the operational area are nonbelligerent.[46]

---

[43] Ibid., 134-6.

[44] The National Academy of Defence of the Republic of Latvia, "Resistance Seminar Series" (After Action Report, Riga, Latvia: The National Academy of Defence of the Republic of Latvia, 2015).

[45] Headquarters, Department of the Army, FM 3-05.130, 1-5.

[46] Ibid., 1-4.

The other extreme is irregular warfare (IW), with the ability to challenge a more powerful adversary. JP 1-02 defines irregular warfare as "a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. IW favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities in order to erode an adversary's power, influence, and will." and underlines that "IW is about people, not platforms."[47] This definition is similar to hybrid warfare in context, hence that is one of the reasons why some scholars argue the existence of the hybrid term.

Unconventional warfare (UW) is now considered as a component part of IW, and defined as "Operations conducted by, with, or through irregular forces in support of a resistance movement, an insurgency, or conventional military operations."[48] This study will further examine the potential of a resistance movement as an augmentation to existing regular capabilities.

In modern conflicts, nations have to consider the different capacities provided by the two extremes of regular and irregular warfare. These methods on their own cannot provide efficient solutions against hybrid threats, but can complement each other to achieve unity of effort.

Resistance Movement

Resistance is one of the ways that can represent the military capacity of the resilience. As discussed previously, the resilience has to have the ability to resist and

[47] Ibid., 1-4 - 1-5.

[48] Ibid., 1-8.

recover from civil, economic, commercial and military shocks.[49] In order to achieve the military goal of resilience, the defense sector must provide instruments to deter military threats, or if deterrence fails, protect the nation`s integrity. Although resilience is defensive in nature, its military aspect has to possess some offensive characteristics.

The resistance movement is an instrument of UW defined as "An organized effort by some portion of the civil population of a country to resist the legally established government or an occupying power and to disrupt civil order and stability."[50] The resistance, such as other irregular or asymmetric warfare, is the tool of weaker countries to compensate for their frailness against a great power. The resistance has a lack of potential to attack other nations, project expeditionary forces, seize territory or completely destroy enemy forces, but possesses vast capability for defensive purposes to exhaust occupying forces.[51] To increase the Hungarian resilience capacity, therefore its defensive capability, the resistance movement is a judicious alternative.

Insurrection, rebellion, uprising and insurgency are not synonyms to resistance. "Rebellion, uprising, or insurrection is a refusal of obedience or order."[52] The insurgency is "An organized movement aimed at the overthrow of a constituted government through

---

[49] NATO, "NATO Summit Guide Warsaw 2016," 131.

[50] Military Factory, "Military Terms," Military Factory, accessed December 11, 2016, http://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4584.

[51] Racz, 20.

[52] John Joseph Lalor, *Cyclopædia of Political Science, Political Economy, and of the Political History of the United States* (Chicago: Melbert B. Cary and Company, 1884).

use of subversion and armed conflict."[53] Because this thesis concentrates on defeating an occupying power instead of established government, the author will use the term "resistance" to describe the organized effort of the civilian population to increase the state resilience capability.

The resistance includes three main elements that can complement each other. The members of the movement are recruited from the civil sector, and historically are a majority of the irregular forces: "Armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces."[54] FM 3-05.130 describes the elements of insurgency, but the resistance also possesses the same components:

Guerillas are the military wing, the most commonly recognized portion of the resistance and conduct paramilitary operations in enemy-held, hostile, or denied territory.[55]

Auxiliary "is the primary support element of the irregular organization whose organization and operations are clandestine in nature and whose members do not openly indicate their sympathy or involvement with the irregular movement."[56] Auxiliary enables the guerrilla force and the underground covertly to survive and function.[57]

---

[53] Military Factory.

[54] Ibid.

[55] Headquarters, Department of the Arm, FM 3-05.130, 4-6.

[56] Ibid., 4-8.

[57] Ibid.

The underground is "a cellular organization within the irregular movement that is responsible for subversion, sabotage, intelligence collection, and other compartmentalized activities."[58] As a clandestine organization, the underground can increase the operational reach of the guerilla forces in areas, which are inaccessible for overt operations.[59]

All the three components are self-sufficient and self-contained, capable of centralized command but decentralized execution, and redundant, in the event that the enemy destroys a portion of the element.[60] Every element crucial to conducting resistance and complements the others in function and in space. Furthermore, these components demand a command element, which supervises and synchronizes the activity, and requires the mass base to provide a passive, but ideological background for the resistance. In order to establish an efficient resistance, all of these separate elements are necessary,[61] therefore recruiting and training only guerillas is not an effective solution, because their effect on the adversary will be very limited.

The resistance movement is a very far-reaching and complicated system. Its traits, such as self-sufficiency, self-contained, centralized command, decentralized execution, and redundancy provide a unique flexibility and survivability for the nation to encounter a stronger foe. The resilience demands very different personal capabilities from its

[58] Ibid., 4-7.

[59] Ibid.

[60] Ibid., 4-6.

[61] Ibid., 4-8.

members. Hence, it can encompass numerous segments of the population, regardless of age, gender, physical capability, and profession.

Historically the establishment of the resistance is a slow process until it is capable functioning effectively.[62] In a gray zone environment the threat will arise without notice, therefore counter hybrid warfare measures have to possess adequate mobilization and readiness ability.

Readiness

The specifics of hybrid warfare, and also the gray zone that blur the borders between war and peace, require an even higher response level from the state`s different stakeholders. The NATO Summit in Warsaw also emphasized the necessity of the Very High Readiness Joint Task Force (VJTF), as a part of the Readiness Action Plan, with decreased readiness time as a military answer to strengthened deterrence and defence posture.[63]

Readiness is the ability of military forces to fight and meet the demands of assigned missions.[64] Logistics, available spare parts, training, equipment, and morale all contribute to readiness. The military recognizes four grades of readiness. At the highest level, a unit is prepared to move into position and accomplish its mission. At the lowest

[62] Ibid., 4-9.

[63] NATO, "NATO Summit Guide Warsaw 2016," 82.

[64] Joint Chief of Staff, JP 1, GL-10.

level, a unit requires further manpower, training, equipment, and/or logistics to accomplish its mission.[65]

However, the readiness time in the new security environment has to consist of non-military segments as well. Their capacity to respond in a short time and therefore their preparation and integration into the state defense plan is as crucial as the readiness of military forces.

Cyber Domain

As the latest recognized domain, the cyber domain does not possess a common definition; each nation and organization has a different understanding of it. The NATO Cooperative Cyber Defence Centre of Excellence applied the Finnish definition:

> Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures.
> Note 1: Representative to the environment is the utilisation of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks.
> Note 2: Information (data) processing means collecting, saving, organising, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions on information (data).[66]

The importance of the cyber domain is increasing continuously because of the electronic information present in the entire spectrum of DIME, hence an adversary can affect the national power through cyber domain. NATO expressed that cyber-attacks are inherent in hybrid warfare, and can be conducted by state and non-state actors in the

---

[65] Jack Spencer, "The Facts about Military Readiness," Heritage, September 15, 2000, accessed November 20, 2016, http://www.heritage.org/research/reports/2000/09/bg1394-the-facts-about-military-readiness.

[66] NATO Cooperative Cyber Defence of Excellence, "Cyber Definitions," accessed January 16, 2017, https://ccdcoe.org/cyber-definitions.html.

context of military operations.[67] In Estonia, the Russian state-sponsored hacker groups conducted a sophisticated and synchronized cyber-attack against the country to interrupt critical services, thereby disrupting and destabilizing the society.[68] The instruments of cyber domain have become more and more dangerous, thus its protection is crucial for nation-states.

The cyber domain is another area in which the nation has to develop resilience. Cyber resilience is defined as "The ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents."[69] The cyber domain demands much more attention in hybrid warfare, hence a flexible solution to protect the DIME power structure.

Limitations

In order to recommend a suitable solution for Hungary against hybrid threats, a complex approach is needed. The threat with its integrated nature is relatively new, and beholders are able to recognize conflicts, where countries are suffering under hybrid warfare. We cannot estimate which state is able to fight successfully against this danger, because the offense is ongoing. We can recognize failures where the new warfare became productive, and we can evaluate the cause of the mistake. Because these are contemporary events, the access to accurate information is limited. NATO and the Baltic

[67] NATO, "NATO Summit Guide Warsaw 2016," 124.

[68] Henrik Praks, *Hybrid or Not: Deterring and Defeating Russia`s Ways of Warfare in the Baltics-the Case of Estonia* (Rome: NATO Research Division, 2015).

[69] NATO Cooperative Cyber Defence of Excellence.

states based their conclusions regarding resilience primarily on the Ukrainian crisis. Forthcoming adversaries can develop different strategies to improve the effectiveness of hybrid warfare in order to offend a state`s stability.

Scope and Delimitations

The study will concentrate solely on Hungary, although other small states have very similar situations, such as Estonia, Latvia, Lithuania, Romania, Bulgaria, Slovakia, Poland, Finland, Montenegro, Moldavia, etc. This study can be adaptable for other small states by adjusting for local differences.

Although the Diplomatic and Economic instruments of national power are also crucial in developing resilience, this study will focus merely on the Military and Information areas. The object of the study is to examine how the state can involve a large number of citizens into the defense sector, utilizing Military and Informational instruments, in order to increase its resilience. The Information portion is the primary means to influence people who will be able to strengthen Military capability. The augmented military capacity results in increased deterrence ability, a message (information) to potential adversaries. The Information instrument consists of the cyber capability that extends the operational reach toward civilians and provides an effective device to influence and command them.

The consequence of recommended changes in Military and Information portions has significant effects on Economy and Diplomacy, but the determination of these impacts demands comprehensive analysis, which is not the purpose of this thesis.

Because of time limitation, the writer cannot examine the possibilities of cyber domain to support resilience showing how it can provide a framework for encryption,

decentralize command and control, provide an ideology to increase patriotism and education and assistance in recruiting members for the resistance.

The researcher does not possess the capability to conduct a well-prepared survey about citizens` willingness to join the resistance and cannot estimate the numbers of potential followers. However, he can provide recommendations for efficient means to acquire their support.

Resistance has several dangers affecting an existing government as well. Due to the time consideration, it is not possible to describe all risks and risk mitigations to overcome these hazards.

Significance of Study

The Hungarian Ministry of Defense, in accordance with the conclusion of the NATO Summit in Warsaw, recognized the importance of resilience, as a significant part of the state`s defense capability. Hungary is committed to increasing defense expenses, encompassing the civil society into the national defense posture and augmenting reserve forces. The way to reach this goal is still under development. Through the analysis of the current security environment and the potential interaction between Military and Information instruments, this study attempts to introduce traditional and non-traditional approaches to expand the options of decision makers, in order to achieve concrete resilience capability.

The involvement of citizenry in the nation`s defense is crucial for a small state, because Hungary cannot maintain a standing professional armed forces large enough to deter a great power. Other small states have already introduced different applications to increase their resilience capability, but there is no best solution, which fits all states. This

thesis examines different nations and their approach to resist hybrid threats against the country sovereignty and integrity, and seeks a solution particularly for Hungary through selection and integration of existing concepts. This study examines the practicability of the interaction of Military and Information instruments of national power, which can reach out and influence the population in order to involve it in the nation`s defense and providing for its own protection.

Resilience is a fairly new notion in modern military scholarship. Efthymiopoulos, in his work about NATO's smart defense and cyber resilience posture said "Resilience as a terminological and operational factor, will become the newest 'brand' and communication name for the Alliance."[70] He also determined flexibility as the most important trait of the resilience.[71] Hungary and other Allies have to examine each other's best practices, concepts and implications in different fields of the hybrid threat in order to assign applications most suitable for an individual country. These applications must address maximum flexibility to the security environment in order to realize authentic resilience. Examination of this topic can offer suggestions for other small states to adapt new defense strategies as well as deliver information about countermeasures in case adversaries apply these regulations.

[70] Marios P. Efthymiopoulos, "NATO Smart Defense and Cyber Resilience," Fletcher, May 2016, accessed January 31, 2017, http://fletcher.tufts.edu/~/media/Fletcher/Microsites/Karamanlis%20Chair/PDFs/Karamanlis_WP_May_2016.pdf, 12.

[71] Ibid.

Summary and Conclusions

The first chapter defined the purpose of the study, and depicted the problem of the possible implementation and importance of resilience by taking advantage of the potentials of Military and Information instruments. The chapter also demarcated assumptions for further consideration, and provided restrictions and scope for examination. Finally, it described the significance of the study, how this work can be beneficial for military scholars. The next chapter will demonstrate those important treatises, which have been written regarding hybrid warfare, NATO`s resilience objectives, and individual states` consideration regarding Military and Information instruments of national power.

CHAPTER 2

LITERATURE REVIEW

Introduction

The purpose of this study is to generate options for the HDF decision makers regarding the Military and Informational instruments of national power, in order to strengthen Hungary's resilience against hybrid warfare.

The second chapter introduces relevant literature that depicts the hybrid threat and introduces counter hybrid warfare solutions. This chapter examines the Russian hybrid warfare against Ukraine, through Racz`s study *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Secondly, the review inspects U.S. practices on special warfare, which will provide another point of view on a great power`s influence on a small state. Thirdly, the literature review examines NATO strategy regarding countering hybrid threats, as a comprehensive approach from the Alliance. Finally, the chapter presents practices of individual states concentrating on the Baltic and Scandinavia. Following paragraphs introduce the most influential literature and authors.

Andras Racz`s work systematically analyzed Russian hybrid warfare in Ukraine in order to identify its characteristics, objectives and prerequisites for success. Racz is a specialist in Russian and post-Soviet security policy, and Senior Research Fellow at the Finnish Institute of International Affairs in Helsinki. His study has been cited several times in NATO papers regarding Baltic hybrid warfare matters. Racz`s work analyzed the

Russian “new generation warfare”, also known as “Gerasimov doctrine”, as a synonym for hybrid warfare, and as the fundamental Russian strategy in the Ukraine crisis.[72]

US special warfare will be another subject to analyze the threat from a great power against a small nation state. Special warfare is “an umbrella term that represents special operations forces conducting combinations of unconventional warfare, foreign internal defense, and/or counterinsurgency through and with indigenous forces or personnel.”[73] From the perspective of this study, unconventional warfare is the most significant aspect of special warfare that the adversary can use against a small vulnerable state. Unconventional warfare (UW) enables “a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power” by influencing “the indigenous population to support the resistance movement or insurgency.”[74] Furthermore, UW occurs in an interagency environment, collaborating with conventional forces.[75] Traits, such as utilizing special operation forces, irregular, and conventional forces in an interagency environment are very similar to the definition of hybrid warfare in chapter 1. Therefore, the examination of UW is relevant to inspect and understand Russian hybrid warfare from a different point of view. The U.S. has a long practice in waging UW in different countries, and therefore possesses a wide range of literature and experience.

---

[72] Racz, 37-38.

[73] Headquarters, Department of the Army, Army Doctrine Publication (ADP) 3-05, *Special Operations* (Washington, DC: Headquarters, Department of the Army, 2012), 9.

[74] Ibid.

[75] Ibid., 14.

The author will use the NATO official position as a benchmark for counter hybrid warfare in the literature review. NATO has paid significant attention in studying hybrid warfare phenomena since the start of the Ukraine crisis in 2014, collecting and synthesizing the ideas of relevant scholars in order to provide an overarching approach to counter the threat. This review will introduce the NATO perception about the near future, utilizing the Alliance`s Strategic Foresight Analysis (SFA).

Individual nations like the Baltic and Scandinavian states–the nations most threatened by Russia–have constructed their own approaches to defend against hybrid warfare. They represent plans, applications or best practices from the standpoint of a small nation, instead of the overarching approach of the entire Alliance. This chapter will also present Hungarian literature as well, regarding identified hybrid threats or planned measures against it.

This literature review will be arranged in accordance with the DIME theoretical framework consisting of four parts. The first part will provide an overall picture of the entire DIME structure and highlight the problem`s interconnected nature. The second part will examine military matters, while the third part will focus on studies regarding the Informational instrument. The fourth part will show those aspects that connect these two instruments and provide recommendations for application. Within each of these four parts, the literature review will be presented according to separate subsections: Russian aggression against Ukraine, U.S. Unconventional warfare, NATO, individual states, and Hungary. At the end of the chapter, the writer will consolidate findings, and underline key themes for further analysis in order to facilitate alternatives for Hungary to counter hybrid warfare.

DIME–Interconnected Approach

Because of the interrelated nature of hybrid warfare, the author will examine the literature that introduces the threat and establishes countermeasures from a coherent perspective. Racz`s study offers a phasing structure to understand the Russian aggression considering the overarching national power approach. U.S. Unconventional Warfare doctrines describe the objectives and the phases of the warfare, and summarize how the U.S. exercises it to influence adversaries. Through the Strategic Foresight Analysis, the review describes those threats that NATO perceives in the future related to hybrid warfare. The documents of Wales and Warsaw NATO Summits offer directives from the standpoint of NATO as a whole. A Finnish policy paper presents a small state perspective through the experience and perception of a Scandinavian country bordering Russia.

Russian Aggression against Ukraine

This section introduces literature regarding the Ukraine-Russian conflict through Racz and Morris thoughts. Racz underlines one particular trait of hybrid warfare that distinguishes it from other known warfare: the single control over the entire DIME structure. Beside the command structure, Racz also analyzed the evolution of hybrid warfare, its operational phases, reasons of effectiveness in Ukraine, and its prerequisites. Morris examines the conflict through Gerasimov`s and Chinese doctrines, looking for similarities between nonlinear and unrestricted warfare and their applications in Ukraine.

Racz`s study collected former and contemporary scholars who examined the hybrid phenomena. Although other authors applied the hybrid term to describe wars in which belligerents utilized irregular, regular warfare and information operations simultaneously such as in Vietnam, Afghanistan, Iraq and Chechnya, these conflicts

lacked "single controlled, well-functioning command structure."[76] Since NATO had not yet applied the term hybrid warfare to the Ukrainian crisis, scholars and journalists used different expressions: non-linear, new generation war, indirect war, full spectrum conflict or special war.[77] Different terms and controversial definitions show that the phenomenon is somehow similar from a historical perspective, but possesses new characteristics as well. Furthermore, that form of hybrid attack has occurred only in Ukraine, so there is no pattern; hence, there is no existing best practice against it.[78]

Racz argued that the primary difference between hybrid war and former warfare is inside the command relationship between military and other stakeholders. "The only really new element was the skillful and effective coordination of the diplomatic, economic, military and information instruments used during the operation, all in the framework of a single, well-functioning command structure."[79] In other words, Russia was able to establish unity of command over different agencies and governmental organizations. In a truly democratic state, the unity of effort is the maximum realizable connection between governmental stakeholders,[80] but Russia, as an autocratic country, can achieve a stronger command and control relationship.

---

[76] Racz, 51.

[77] Ibid., 37-41.

[78] Ibid., 12-13.

[79] Ibid., 51.

[80] Joint Chief of Staff, JP 1, GL-13.

In order to understand the dynamics, objectives, and the interconnected nature of hybrid warfare, Racz sequenced its progress, and identified three main phases from the aggressor perspective: Preparatory, Attack, and Stabilization phases.

The preparatory phase of hybrid war consists of the traditional measures of Russian foreign policy. These measures are "not explicitly or necessarily illegal, which makes it hard for the target country to defend itself against them."[81] In other words, every instrument of Russian foreign policy can be a potential preparation for a future hybrid intervention. In order to avoid a targeted country`s active countermeasures, the violence is covert, and under the political or legal thresholds. The preparatory phase has three sub-sections: strategic, political and operational preparation.

Strategic preparation explores the vulnerabilities in the state administration, Economic and Military instruments of national power; establishing networks of loyal Non-Governmental Organizations (NGO); gaining influence in media channels in the targeted country; also influencing international audiences.

Political preparation encourages dissatisfaction with the central authorities; strengthening local separatist movements and fueling ethnic, religious, and social tensions; isolating the targeted country by informational measures; bribing key politicians, military and administrative officials; offering profitable contracts to oligarchs and business people; establishing connection with criminal elements.

[81] Racz, 59.

Operational preparation launches coordinated political pressure and disinformation actions; mobilizing officials, officers and local criminal groups; mobilizing the Russian armed forces under the pretext of military exercises.[82]

The preparatory phase involves all elements of national power to shape the strategic and operational environment inside the targeted country, in the aggressor country, and influences international audiences as well, while prepositioning military potential to the targeted area. The aggressor also gathers potential proxies from ethnic, religious and political groups; establishes connections to officials, NGOs and criminal groups in order to gain information and decrease the effectiveness and legitimacy of the existing government.

The attack phase starts when the first phase established preferable conditions in the security environment to launch the full-scale hybrid offensive. This phase ends, when the aggressor achieves its goals, the attack is culminated or the invader has to change from hybrid warfare to an open armed conflict. Successful hybrid attack is a short duration operation. The operation achieves its objective when the central government acknowledges its lost control over the territory and the armed hostility is terminated.[83] The attack phase also has three sub-sections: exploding tensions, ousting the central power from the targeted region, and establishing alternative political power.

Exploding tensions sub-section organizes massive anti-government protests and riots; infiltrating Special Forces disguised as local civilians to seize administrative

[82] Ibid.

[83] Ibid., 59-64.

buildings; weakening the position of the central government by sabotage and provocation, using proxies and criminal elements; launching disinformation campaign by media; maintaining the opportunity of conventional offensive in case of a targeted country`s counterattack.

Ousting the central power from the targeted region sub-section helps disabling the central power by capturing key infrastructures; blocking the central power's media; establishing communication and information monopoly; disabling the local armed forces by non-lethal means; misleading and disorientating the international audience, and discrediting the target country.

Establishing alternative political power sub-section assists declaring an alternative political center; encouraging separatism; strengthening the legitimacy of the new political bodies by media and diplomacy; and alienating local population from the central power.[84]

This phase also takes advantage of the synergic effect of offence by Military, Information, and Diplomatic instruments. The shaping operations in phase one prevent the possibility of effective countermeasures by the legitimate government. The aggressor maintains the possibility of a large-scale conventional operation in case of counterattack against invading forces. The primary objective of this phase is to separate the central government from the population mainly by informatics and diplomatic tools.

The stabilization phase starts when the armed conflict is over, and the targeted country`s government has lost control over its territory. The phase ends, when the aggressor legitimizes its rule. The central government cannot commit open conventional

[84] Ibid., 61-63.

attack against the overpowering aggressor. The sub-sections of stabilization phase are political stabilization of the outcome; separation of the captured territory from the target country; and lasting limitation of strategic freedom of movement of the attacked country.[85] The author will not analyze this phase in detail, because mainly diplomatic instruments exist in this phase and the counter hybrid warfare has to concentrate on the first and second phases in order to prevent the stabilization phase.

Morris examines the Gerasimov doctrine through modern Chinese doctrine to elucidate the Russian hybrid or by Gerasimov`s term nonlinear warfare`s application in the Ukraine-Russian conflict. He argues that nonlinear warfare contains similarities to the Chinese unrestricted warfare but also has historical roots in previous Russian doctrines. "Both strategies involve using proxies and surrogates to not only exploit vulnerabilities in low intensity conflict, but to also prepare for future operations that may involve high intensity conflict"[86] in order to reach long-term political outcomes. Therefore, nonlinear warfare aims to achieve political goals favorable for Russia in gray or black zones as well. This warfare directly or indirectly employs diplomats, intelligence agencies, professional soldiers, Special Operation Forces, insurgents, guerillas, extremist groups, mercenaries, and criminals.[87]

In order to realize desired strategic orientation and geopolitical outcomes, primary through non-military approaches, the applied doctrine must be supra-national, supra-

[85] Ibid., 64-66.

[86] Morris.

[87] Ibid.

domain, supra-means, and supra-tier. In the Ukrainian case, supra-national condition extends the range of a state against state conflict to a NATO, EU, and Eurasian Economic Union problem, involving national, international and non-state organizations. Russia combines all domains including cyber in order to maximize the effect of media and fabrication, cultural, psychological, and network warfare. "Supra-means combinations unite aspects of military and non-military means,"[88] through destabilization, deception, information operation, and limited military intervention phases, while maintain local population support. Russia`s Ukraine campaign confuses tactical, operational, and strategic levels of war, while applies conventional and unconventional operations in order to achieve supra-tier condition.[89]

These phases and their content provide a better understanding about the runoff of hybrid war, also about its objectives. Both Racz`s and Morris's studies emphasize that Russia employs its centralized DIME power in a synchronized attack against the vulnerabilities of the entire Ukraine DIME structure in order to achieve synergic effects and divide defensive efforts.

U.S. Unconventional Warfare

Through UW, the literature review examines how U.S. Special Operation Forces can leverage the nation`s DIME structure in order to maximize the effect of UW over an adversary. The review also introduces the UW`s phasing structure, main objectives in different stages and prerequisites for successful UW operations.

---

[88] Ibid.

[89] Ibid.

The unity of effort is a key element to facilitate coordination and ensure efficient use of all available resources during conducting UW. As most of Special Operations (SO), unconventional operations "occur in an interagency environment in which the U.S. Government departments and agencies are working toward common national objectives."[90] The interagency environment is crucial in UW, because "The objective of UW is always inherently political,"[91] and therefore needs other agencies to pursue diplomatic goals beyond military ones. As it was aforementioned, the unity of effort offers a weaker control over resources than unity of command, thus the Military instrument of national power is not able to exercise command authority over other interagency organizations to realize the highly integrated design.

UW operations` phasing structure assists understanding the concept and sequencing how UW affects adversaries. UW consists of seven phases:

Phase 1. Preparatory: Concentrate on understanding the operational environment, planning, and conducting interagency shaping operations in order to "create or affect local, regional, and global conditions that are beneficial to future UW operations."[92] Starting with this phase, military intelligence support operations (MISO) continuously discredit the existing government, strengthen friendly civilian support for insurgency

[90] Headquarters, Department of the Army, ADP 3-05, 1-14.

[91] Headquarters, Department of the Army, FM 3-05.130, 3-9.

[92] Ibid., 5-01.

movement, introduce a shadow government, and maintain support of the indigenous populace for U.S.[93]

Phase 2. Initial contact: Special Operation Forces (SOF) establish contact with irregular element.

Phase 3. Infiltration: SOF units infiltrate to UW area of operation.

Phase 4. Organization: Development of capabilities of irregular force and the resistance movement.[94] Civil Affairs units provide local resources, facilities and support the resistance movement, maintain contact with friendly local agencies and civil authorities, and minimize the effect of UW operations on civilians.[95]

Phase 5. Buildup: Expansion of resistance capabilities in order to conduct operations to meet mission objectives.

Phase 6. Employment: Irregular forces increasingly operate in the UW area of operation to achieve mission objectives. Irregular forces can operate independently as decisive operation, or in support of conventional forces as shaping operations.

Phase 7. Transition: In this phase, the invading forces consolidate their gains and assist the host nation in reconstruction. This form of stability operation helps the new government to maintain its legitimacy.[96] Civil Affairs plays a major role in the integration of interagency, inter-governmental and non-governmental organization in

---

[93] Ibid., 6-01.

[94] Ibid., 4-05.

[95] Ibid., 7-05.

[96] Ibid., 4-10.

order to stabilize the new government and the capability of its security forces.[97] The next paragraph identifies the three prerequisites of U.S. UW operations.

The United States has defined three prerequisites for successful UW operations: 1. A weakened or unconsolidated government or occupying power; 2. Segmented population, 3. Favorable terrain. Because it is extremely difficult to organize resistance under a fully consolidated government or occupying power, the given or prepared conditions for weak government is preferable for UW. There must be a significant population that is against the existing government or occupying power and has the will to fight against it. Starting with the preparation phase, this unsatisfied population is able to grow, thus providing support for the resistance movement. Resistance requires physical and human terrain that provides safe haven and security to train, reorganize and recuperate. Physically favorable terrains can be mountains or jungles but also artificial safe havens such as urban ghettos or international borders.[98]

UW applies the nation`s entire DIME structure to achieve the desired end state over an adversary. In order to do so, SOF have to maintain interagency coordination to realize unity of effort among stakeholders. During the execution of UW, SOF also have to reach out to interagency resources and support to complete successfully the 7 phases. MISO and Civil Affairs units have significant roles to influence local and international target audiences, and to assist consolidating gains. SOF also can conduct UW in order to

---

[97] Ibid., 7-09.

[98] Headquarters, Department of the Army, Training Circular (TC) 18-01, *Special Forces Unconventional Warfare* (Washington, DC: Headquarters, Department of the Army, 2010), 1-4.

facilitate the success of conventional forces. The three prerequisites for successful UW operations help to understand those vulnerabilities that an aggressor can take advantage of to enable resistance movements.

After the general examination of the threat from the Russian hybrid and U.S. UW perspective, the next part will inspect NATO and Finland, and their approach countering the threat.

NATO

The NATO Strategic Foresight Analyses (SFA) describes the near future, as "Former Soviet territory and neighboring countries will remain susceptible to Russian political, economic, and military pressure and other elements of the hybrid threat."[99] SFA underlines that Russian actions can become more assertive towards neighboring regions while hybrid aggression remains under the threshold to trigger collective response. NATO began to align its capabilities to be adequate in the forecasted future and, during the Summits in Wales and Warsaw, provided counter hybrid threat directives to its members. SFA documents expressed the urgency to revise the NATO decision-making process to respond under Article 5 threats.[100] NATO recommendations and implications for counter hybrid warfare are beyond the limit of merely military means, and consist of Diplomatic, Economic and Informational instruments as well.

---

[99] NATO ACT, "Strategic Foresight Analysis 2015 Update Report," 2015, accessed January 27, 2017, http://www.act.nato.int/images/stories/media/doclibrary/160121sfa.pdf, 7.

[100] Ibid., 10.

The NATO Wales Summit 4-5, September 2014 intended to find immediate solutions against the threat from Russia. The Ukrainian crisis forced the Alliance to revise its strategy and initiate diplomatic and military countermeasures against the hybrid threat. The key military outcome of the Summit was the Readiness Action Plan including a Very High Readiness Joint Task Force (VJTF), which provides a more responsive, better-trained and better-equipped force to respond to the changed and broader security environment. The Summit also recommitted to the Article 5 collective defense commitment, and emphasized the importance of Article 3, the individual and collective capacity to resist armed attack. Members also agreed to increase military spending to satisfy their Article 5 and 3 obligations. On diplomatic grounds, NATO "suspended all practical civilian and military cooperation with Russia, while leaving channels open for dialogue on the situation in Ukraine."[101]

NATO reassured east and central European members of its commitment to collective defense against Russian aggression, as well as offered assistance in capability and interoperability building to facilitate the members` Article 3 requirements. NATO objectives remained military centric in the Summit. The increased GDP percentage on defense spending and the reassurance of the Alliance reflects a military focused approach. The recommendation to increase cyber capability and the suspended cooperation with Russia indirectly also related to a military response. The Alliance has achieved significant results in the mentioned areas in the following two years; hence, the next Summit was able to set new objectives to extend ways and means.

[101] NATO, "Wales Summit Declaration," 2-3.

Warsaw NATO Summit, 8-9 July 2016, also set the priority on Russian aggression. The Summit underlined the achievement of the Alliance regarding the fight against hybrid threat. NATO defines the key countermeasures as deterrence and defense. The strengthened deterrence and defense posture includes increased response capability: the Readiness Action Plan; conventional forces; forward presence; joint airpower and maritime forces; cyber defense; civil preparedness and countering hybrid threats in cooperation with the EU.[102] Diplomatic and economic cooperation with the EU includes energy security issues, coordinated cyber defense, supporting partners in defense capacity building, increasing maritime security and improving readiness by joint military exercises.[103] All of these endeavors show a much wider approach than a principally military solution, and attempt to affect Alliance Diplomatic, Informational and Economic potentials as well.

The Summit applied the resilience, a different approach against hybrid threats, in order to intensify members` contribution in collective defense efforts. "Under Article 3 of the North Atlantic Treaty, all Allies are committed to building resilience, which is the combination of civil preparedness and military capacity."[104] The maintained and developed individual and collective capacity to resist armed attack, is related to the society`s ability to resist or recover from shocks. These shocks can be the combination of civilian, economic, commercial and military factors. "Allies agreed to baseline resilience

[102] NATO, "NATO Summit Guide Warsaw 2016," 53-54.

[103] Ibid., 286.

[104] Ibid., 131.

requirements in seven strategic sectors–continuity of government, energy, population movements, food and water resources, mass casualties, civil communications and transport systems."[105] Nations have to develop the capability to provide these services for assisting NATO forces, even under the pressure of an armed attack. "To deter or counter potential threats or disruption to the civil sector, effective action requires clear plans and response measures."[106] In order to ensure continuous services, nations must be prepared to protect their civil sectors. The Summit highlighted the need to complement military efforts with robust civil preparedness to achieve resilience, hence support Article 3 demands. The Conference underlined that a nation can develop resistance through home defense, cyber defense and medical support. Members of the Alliance that are well prepared are less likely to be attacked.[107] In other words, resilience is a deterrence capability.

NATO identified the hybrid threat as one of its main priorities during NATO Summits in Wales and Warsaw. NATO SFA also acknowledged the hybrid warfare as a long-term threat against NATO and its partners. NATO Summit in Warsaw developed further countermeasures in order to extend the Wales Summit`s mainly military focused outcomes. Therefor the Warsaw Summit involved more Diplomatic, Economic and Informational instruments to strengthen the Alliance deterrence and resilience capability.

[105] Ibid.

[106] Ibid.

[107] Ibid.

Individual States

Finland already has experience in countering hybrid threats and building resilience because of its close proximity to Russia. Finland also has recognized the opportunity of resilience: "Building societal resilience is the only assured way of keeping at least some of the home-field advantage because the aggressor will try to build up and utilize the effect of surprise. This, however, is not an easy task. It requires a long term plan and dedication to implementation."[108] Aapo Cederberg and Pasi Eronen, in their policy paper, defined the hybrid threat as "mobilisation of all national means to achieve political goals."[109] It underlines the significance of strong political leadership to achieve unity of command over these instruments. Their approach also originated from examination of the Ukraine conflict much as NATO scholars did. They argued "Western liberal democracies are limited in their capabilities to wage hybrid war to its maximum, particularly during a time of perceived peace."[110] Therefore, autocratic regimes have the advantage due to their centralized decision-making, which is not limited to normal checks and balances. The policy paper used the "hybrid defense" term to describe a comprehensive defense approach as a possible option for a small state against hybrid attack. Because small states lack resources, political agenda, wide intelligence apparatus and appropriate military power, they have to apply new security strategies. Instead of settling with a classic intergovernmental approach, the authors suggested intersocietal

[108] Cederberg and Eronen, 8.

[109] Ibid.

[110] Ibid.

security as a solution. The intersocietal approach means that the whole society should be engaged in defensive efforts, and it demands clearheaded vulnerability analysis, reliable intelligence, and robust counterintelligence efforts.[111] The writers offered the following proposals to organizing hybrid defense:

1. Develop a credible defensive posture against hybrid threats that cannot be based solely on security forces, but on joint action of all stakeholders in society including also representation from civil society and the private sector;

2. Emphasize the importance of political leadership because of the necessity of collaboration between several sectors;

3. Ensure shared understanding of security and shared security awareness among stakeholders;

4. Encourage the society to find the vulnerabilities and to apply countermeasures to protect them;

5. Create competent intelligence and counterintelligence capacity;

6. Mitigate the effect of disinformation via cyber domain and media;

7. Garner international collaboration.[112]

The Finnish approach aligns with the NATO resilience endeavor but provides a more detailed and extended objective. It originated from their experience that had continuous pressure from Russian hybrid warfare. The policy paper recommended several objectives to organize hybrid defense. However, there was no precise

[111] Ibid.

[112] Ibid.

recommendation as to how a state can involve the society to augment its security. Although this Scandinavian country is not a NATO member, as a small state and an experienced nation in building resilience, the Finish understanding and their best practices are important for other small countries, like Hungary.

Using this interconnected approach, the literature review introduced hybrid warfare from the Russian perspective in Ukraine, and from U.S. UW. The author examined how these two approaches exercise control over DIME power for efficient use of resources. In order to understand the two warfare`s dynamics and sequencing, the review inspected their phasing structures. NATO Summits realized the danger of hybrid warfare and worked out countermeasures to overcome the threat. Conventional forces, increased response capacity and forward presence ensure a deterrence capability against open armed aggression. NATO conferences also emphasized the importance of cyber defense, resilience involving civil preparedness, and coordination with the EU, which are beyond the military. The Finnish report highlighted the resilience capability parallel to the hybrid defense, which can be an effective response for a small state. The resilience also offers potential to involve a large number of citizens with different capabilities, interests and skills. The next section provides insight into the Military instrument of national power regarding hybrid environment.

Military Concerns

This section of the literature review examines the lethal segment of hybrid warfare. In order to do so, the review describes the Ukraine-Russian conflict and how the military superiority affected the operation. Then this section introduces the U.S. UW position, and shows how the U.S. employs military power in UW area of operations to

achieve lethal effect with or without the support of conventional forces. NATO`s primary instrument to counter the hybrid threat is the conventional response capability in order to compensate for hostile military superiority. The author describes NATO`s lethal military preparation against hybrid attack. Than the literature review presents an unconventional approach to strengthen a small nation`s deterrence capability, and points out the significance of a proper legal framework to enable military forces to intervene timely and adequately. Finally, it introduces the recent capability of the HDF.

Russian Aggression against Ukraine

This section examines the Ukrainian conflict through Racz`s and Morris`s works. Racz identified military superiority as a prerequisite of the Russian success in the annexation of Crimea. The Russian conventional forces at the international border provided deterrence capability against Ukrainian security forces, and prevented immediate Ukrainian military response. In the East Ukraine case, the Russian conventional forces were able to intervene effectively in order to support separatists against advancing Ukrainian troops. Morris highlights the importance of non-traditional warfare plus the role of Russian superior conventional equipment and weapons of mass destruction, as a source of deterrence, in the conflict.

Racz observed two separate hybrid operations in the Ukraine conflict. The first was the annexation of Crimea between 20 February 2014 and 19 March 2014, which was successful, thus Russia achieved its objective in phase two and consolidated its success in the stabilization phase. The second was in East Ukraine, starting at 6 April 2014, which was partially successful, but the central government was able to launch a counteroffensive, and the majority of the population maintained their support towards

Kiev. In that case "the initially hybrid war was transformed into a conventional, but limited armed conflict."[113] However, both demanded the existence of Russian regular military superiority.

In order to gain military dominance, Russia possessed a technologically advanced armed force compared to Ukraine, mobilized and prepositioned covertly to the operation area. Racz argued that "The reason why Russian military superiority is essential is that the ability of the attacked country to conduct armed resistance needs to be disabled in order to allow Phase 2, namely open, armed actions to unfold."[114] In other words, if the aggressor does not have military superiority, the proxy force and its Special Forces enablers would be overwhelmed by local security forces and conclude the conflict. In the Crimea, Russian forces lined up along the border and threatened Kiev by an intervention with massive conventional power. In the case of Ukraine, Russia committed its security forces against the separatists.[115]

Russia effectively used Special Forces (SF) in order to organize riots in Crimea and to establish insurgency in East Ukraine. SF, as a force multiplier, were able to consolidate dissatisfied peoples and organized crime groups and lead them to conduct riots, occupy key administrative buildings, infrastructures and military installations while denying official involvement in the conflict.[116]

---

[113] Racz, 73.

[114] Ibid., 75.

[115] Ibid.

[116] Ibid., 63.

In the East Ukraine case, Kiev recognized that Russia wanted to avoid an open full-scale armed conflict due to the anticipated high political costs, and therefore initiated anti-terrorist operations against the SF led separatists and realized significant success. Russian conventional force had to intervene and support separatists to secure its gains. The aggressor was not able to realize the same outcome as in Crimea. It had to sacrifice the covert presence, and became involved in a long-term conflict. However, without its military superiority Russia could not maintain the support to the separatist, hence would suffer defeat in this region.[117] Racz also underscored the logistic as another prerequisite for the success in Ukraine, which provided sufficient support for Special Forces units and proxies, and enabled long-term presence for regular forces along the border.[118]

Morris highlights the importance of Russian unconventional warfare in the Ukrainian conflict. Unconventional operations aid Russia to undermine the legitimacy of the Ukraine central power by avoiding Ukrainian conventional forces while eroding the country`s power and will through use of indirect, hence non-traditional approach. He also underlined the significance of military superiority as a success criterion such as conventional military equipment and weapons of mass destruction.[119]

In both examined cases in Crimea and East Ukraine, the existence of military superiority was crucial to enable, maintain and secure the results of hybrid warfare. The aggressor had to be technologically advanced and superior in strength to deter or defeat

[117] Ibid., 75.

[118] Ibid., 82-83.

[119] Morris.

the targeted country`s counterattack. The capability of regular conventional and SF, as well as the logistical capacity of the aggressor, were crucial prerequisites for the hybrid offensive.

U.S. Unconventional Warfare

In order to understand an adversary`s potential lethal military effect on a country in a hybrid environment, the literature review will inspect U.S. Special Operations doctrines. The author will examine Special Operation Forces` force multiplier capability, their role in covert lethal military operations, and the SOF collaboration with conventional forces.

The primary role of SOF in UW is to advise, train and assist indigenous and paramilitary forces, thus serving as force multipliers in order to pursue mutual military objectives with trained local forces. SOF can realize these security objectives with minimum U.S. visibility, risk, and cost.[120] In other words, a relatively small SOF element can generate a large irregular force, and "reinforce and enhance the effectiveness, legitimacy, and credibility of the supported foreign government or group"[121] with and through partner nation forces.

SOF is able to conduct UW unilaterally or in support of conventional forces,[122] with or without the anticipation of large-scale U.S. military involvement. In a general war scenario, UW focuses largely on military aspects in order to make them more vulnerable

[120] Headquarters, Department of the Army, ADP 3-05, 1-14.

[121] Ibid.

[122] Headquarters, Department of the Army, FM 3-05.130, 4-10.

to the pending introduction of conventional invasion forces. Meanwhile in limited war, U.S. SOF conduct covert UW operations with proxies to realize political objectives. U.S. conventional forces possess and are able to provide overwhelming military superiority in a targeted country in a general war scenario. The U.S. operational reach extends the capability and capacity of conventional and SOF forces in order to "multiply forces available and provides increased options for defeating adversaries."[123]

SOF have a unique force multiplier characteristic, which enables UW operations to increase the legitimacy of a supported government through and with indigenous forces. When U.S. SOF conduct UW in support of conventional forces, the SOF can take advantage of the overwhelming military superiority and operational reach of U.S. regular formations. Through the Russian and U.S. literature review, the author examined the lethal military perspective of the aggressor. The following part will focus on countermeasures for how the Alliance can assist its members, and how individual states can prepare for hybrid threat.

NATO

NATO SFA predicted a future in which the hybrid challenges will lessen the importance of purely military solutions in resilience capability. The document identified "power politics" as a returning trend; however, "This trend should include all aspects of power not just hard power."[124] The Military instrument of national power becomes a supporting effort that complements other elements, but is not likely to utilize itself in

[123] Ibid., 1-5.

[124] NATO ACT, "Strategic Foresight Analysis 2015 Update Report," 9.

order to facilitate power politics. After the annexation of Crimea, the Alliance initially concentrated on strengthening primarily conventional forces to regain the deterrence capability against Russia on a traditional warfare basis. One part of this effort was the establishment of VJTF in accordance with the Readiness Action Plan to provide a larger and quicker reaction capability in and around NATO territory.[125] Forward presence was another portion of deterrence. Positioning NATO troops in Baltic states, Poland and Romania reassures the collective defense posture for countries on the periphery of the Alliance and sends a warning to the aggressor.[126] Although the nuclear deterrence and ballistic missile defense are a vital part of deterrence, they are beyond the scope of this study.

The NATO response capacity consists of two parts: the NATO Response Forces (NRF), and the VJTF. NATO Response Forces have land, maritime, air and special operation forces components, and now consist of about 40,000 soldiers. VJTF, the NATO "spearhead force" of "around 20,000, of which about 5,000 are ground troops, is now operational and is ready to deploy within days wherever it is needed."[127] These two response capabilities together can project around 60,000 soldiers into a single crisis area, which is a significant power to deter aggression, if they arrive in time and are not divided among different crisis hotspots.

[125] NATO, "NATO Summit Guide Warsaw 2016," 82.

[126] Ibid., 83.

[127] Ibid., 82.

NATO`s emphasis on increased readiness capacity supports Monaghan`s views on future military conflicts. Monaghan inspected the Russian new generation warfare, through Gerasimov`s doctrine, and underlined the importance of readiness in the hybrid war: "At the outset, he suggests that in the twenty-first century, we have seen a tendency towards blurring the lines between the states of war and peace. Wars are no longer declared."[128] Therefore, every traditional or non-traditional military solution against hybrid warfare of the Alliance itself or of its members has to possess high readiness forces.

NATO established tactical command posts for peripheral members to facilitate mission command and the rapid deployment of VJTF and Allied follow-on forces. The NATO Force Integration Units will operate in the Baltic states, Bulgaria, Poland, Romania, Hungary and Slovakia. NATO also developed deployable main command post capability as a high-readiness multinational corps headquarters.[129] These new capabilities can enforce not just the cooperation and integration of host nations into NATO system, but can facilitate the decision-making process to react promptly to a hybrid attack. The planned establishment of logistic headquarters, in accordance with prepositioning of equipment and supplies, enables the sustainment of response forces against imminent threats.

---

[128] Andrew Monaghan, "Putin's Way of War," *Parameters* 45, no. 4 (Winter 2015-16): 71, accessed November 20, 2016, http://strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf.

[129] NATO, "NATO Summit Guide Warsaw 2016," 83.

Threatened Allied countries still need to develop their own capabilities against hybrid aggression; the NATO collective defense capability is not an ultimate solution to counter the hazard. Individual countries need to have their capability to fight under Article 5 threshold, and extort open armed conflict to allow collective defense, and simultaneously enable and support NATO operations.[130] In other words, resilience is a shaping operation that creates the conditions for VJTF, NATO Response Forces and follow-on forces to project military power into the attacked country.

Individual States

From the view of individual small states, the literature review highlights two important military considerations: the first is the potential role of resistance movement in defense strategy, and the second is the alignment of the judicial system to the hybrid threat. During Baltic resistance seminars, participants examined the potential of resistance movement in small states` defense strategy. Estonia denoted the significance of Rules of Engagement – the legal rationale for fighting against hybrid warfare.

The Baltic resistance seminar examined the potential of the resistance movement in the national defense strategy. The seminar directly connected the resilience and the resistance movement showing that the resilience is the instrument defending the nation`s sovereignty, while the resistance is the tool to regain it. The participants of the seminar argued that resistance can be a determining factor in the fight against hybrid threats, but underlined the importance of readiness, thus the necessity of preparation for resistance

[130] Ibid., 131.

before open or covert military engagement.[131] The resistance movement and its armed capability need time for mobilization and have to have acceptable readiness capability, but peacetime preparation can provide aid to achieve adequate response capacity.[132] The bottom line is that the resistance movement, thus irregular warfare, can be a significant portion of deterrence and because of the involvement of wide range of citizenry enables another link to the population. The Military and Information part of literature review will further examine this opportunity.

Estonia recognized the importance of the adjustment of its judicial system to the new security environment. Response to "little green men," terrorist or civil mobs requires a detailed legal background, which provides intent and decision-making authority for security forces.

Countering terrorism is an important segment of NATO capabilities in the Warsaw summit.[133] From a hybrid warfare view, terrorist elements can augment regular, irregular and criminal components of invading forces. The government`s inability to counter terrorist activities can ignite passions to confront reigning political entities, thereby further weakening its power. Racz highlighted that the main goal for hybrid warfare is to weaken the legitimacy of the existing government, therefore weak governments cannot resist successfully against hybrid attack.[134] The other part of

---

[131] The National Academy of Defence of the Republic of Latvia, 5.

[132] Ibid., 3-5.

[133] NATO, "NATO Summit Guide Warsaw 2016," 118.

[134] Racz, 59.

countering terrorist activities is connected to the "little green men" phenomena, thus how the state legal system can handle threats other than open armed conflicts.

Russia took advantage of the shortfalls of the Ukrainian legal system, because the government was not able to manage the situation in Crimea with its existing statutes. Soldiers of the Russian Special Operation Forces were declared as nice "little green men," at the commencement of the annexation of Crimea. Ukrainian decision makers, and their security forces were not sure how to respond to soldiers without insignia and against civil mobs when they were threatening governmental and military installations. When security forces finally received orders, it was too late to intervene in the situation. The key problem here is the proper legal framework that provides the authority for decision makers to issue timely orders to designated forces for intervention.[135] Estonia recognized the necessity to fight back immediately, and adjusted its legislation to enable appropriate countermeasures.

The commander of Estonian Defense Forces declared "when the first Little Green Men appear they will be shot at. Any armed man without insignia will be considered a terrorist and will be dealt as such."[136] Other members of the Alliance have to adjust their legislation to enable security forces to fight against "little green men" immediately because time is crucial in hybrid war. Like Estonia, other states also must increase unity of effort by establishing clarity between line of command and responsibilities of internal security forces and armed forces. The real terrorist threat of hybrid war still demands

[135] Ibid., 91.

[136] Praks, 9.

counter terrorist capability, but the “little green men” phenomena requires a very similar approach.[137] Parallel to Estonia, in December 2014 Lithuania also amended their statute on the use of military force, in order to authorize the use of weapons by the armed forces in the defense of the state`s territory in the event of threats other than armed aggression.[138] States have to deter an aggressor by having the willingness, correct decision-making process, unity of effort and updated Rules of Engagement to react immediately. The next section of the literature review introduces the recent Hungarian military capability through the view of the Prime Minister, a NATO sponsored analysis, and the Fundamental Law.

Hungary

Prime Minister Viktor Orban, during an interview in the Katolikus Radio on 29 October 2016, depicted the current capability and the intended development of HDF. Orban expressed that the military had not been the priority previously, but now realized economical improvements would promote the development of the defence sector. Neighboring countries are investing in their military and conducting rearmament, but Hungary is the last in the region to do this. However, Hungary needs a more capable military. Compulsory conscription is not a solution because of bad experience with this system in the past, and Hungarians do not like it if something is mandatory. The Prime

[137] Ibid.

[138] Piotr Szymanski, “The Baltic States’ Territorial Defence Forces in the Face of Hybrid Threats,” OSW, March 20, 2015, accessed March 21, 2017, https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-03-20/baltic-states-territorial-defence-forces-face-hybrid-threats.

Minister communicated that he is not happy about the current condition of the HDF and that the government will invest in the military and improve the capability of the volunteer territorial based reserve force.[139]

In a NATO sponsored study *Newcomers no more? Contemporary NATO and the future of the enlargement from the perspective of post-cold war members*, Peter Marton and Peter Wagner wrote a chapter examining the Hungarian military capability, foreign policy, and popular opinion about security matters.[140] They underline that NATO membership is vital for Hungary, a small and relatively poor Western country, in order to maintain its autonomy and independence.[141] Hungary`s basic preference is to have a peaceful milieu in the region, including a none-too-confrontative relationship with Russia. Prime Minister, Orban expressed that Hungary is committed to collective defense but not to economic sanctions against Russia.[142] Marton and Wagner depicted the strength of HDF in 2010 as 26,000 officers and enlisted members and 3,500 people in the Ministry of Defence, and assumed 3,000 unfilled positions.[143] Furthermore, because of the underfinancing of the military, the human and technical resources were depleted.[144] The public sees Hungary as a toy of great powers. Citizens do not easily become directly

[139] Viktor Orban, Inteview with Viktor Orban.

[140] Marton and Wagner, 137-160.

[141] Ibid., 145.

[142] Ibid., 151.

[143] Ibid., 143.

[144] Ibid., 144.

relevant in the field of foreign policy. A poll in 2015 declared that 36 percent of the population is not interested in foreign or security policy matters.[145]

Marton and Wagner identified only a few areas, where the HDF improved between the NATO membership in 1999 and 2015. They highlighted the establishment of Special Operation Forces that provided a new capability and were tested in Afghanistan under U.S. command.[146] During NATO and EU missions many Hungarian service members gained experience in the international environment. The Province Reconstruction Team mission in Afghanistan was unique, where Hungary utilized the "whole of government" approach and the unity of effort work.[147]

The Hungarian Parliament resolution 35/2016 (XII.19) maximizes the personnel of HDF. The authorized strength is 5,690 officers, 9,270 NCOs and 8,850 enlisted, overall 23,810 soldiers. The resolution also maximizes the number of volunteer reservists at 8,000 soldiers.[148] In reality, these positions in active duty and reserve forces are not completely filled up, but the actual number is restricted. In order to employ its small military capability at the right time, Hungary modified its legislation to increase the response capability against an immediate threat.

The Hungarian Parliament adjusted the Fundamental Law to the intensifying terrorist threat in order to enable immediate military intervention in case of terrorist

---

[145] Ibid., 146.

[146] Ibid., 141.

[147] Ibid., 144.

[148] Parliament of Hungary, "35/2016. (XII. 19.) OGY határozat," *Magyar Közlöny* no. 208 (December 19, 2016): 82616-82790.

attack. The sixth modification of the Fundamental Law on 26 April 2016 provides wider instruments for the political decision makers to use against sudden terrorist actions. The government is able to involve special military capabilities in order to augment police forces and national security services.

While military power lost its preeminence in hybrid warfare, it still is the primary instrument to deter conventional armed threats and to prevent the escalation to a full-scale open armed conflict. This section of the literature review pointed out that military superiority is crucial in a hybrid environment. It is crucial for the aggressor despite the direct involvement of conventional forces being limited. Military superiority enables SO in occupied territories by supporting those with conventional capabilities while deterring large-scale counterattacks. It is also critical for NATO to rapidly project forces into the threated are in order to compensate for the adversary`s superiority and to deter follow-on operations. However, NATO needs the aggressor to overstep the collective defence threshold during its hostile actions. Under this threshold or until NATO response forces arrive, the targeted country has to utilize its own military capabilities. The resistance movement, hence irregular warfare, has a unique potential to deal with military superiority or to project deterrence. The Estonian example underscores that the synchronization of the legal system is crucial in order to counteract hybrid attacks in time. Therefore, the military capability is meaningless, if the nation cannot use this force in the right time and with full expediency. Hungary, however needs significant investment in the military and already has adjusted its legislation in order to increase the response ability of the HDF. The next part of the literature review concentrates on the Informational instrument of the nation`s power.

Informational Concerns

Regarding to the Informational instrument of national power, the literature review will inspect three different functions: information protection, intelligence, and influencing. The review will examine these functions on the human terrain and on cyber domain as well. This part presents informational concerns through the inspection of the threat in the Ukraine conflict and by U.S. UW practices, and through recommended solutions by NATO and individual countries. Additional sources will introduce theories on influence warfare and weaponized information in order to understand the threat inside information. Finally, the review will present Informational Warfare from the perspective of Hungary.

Russian Aggression against Ukraine

In order to understand the potential effect of an adversary on a small state through the Informational instrument of national power, the author will study the Ukraine conflict. Russia applied a broad scale of information operations to identify Ukraine vulnerabilities, to manipulate the government, the international community and the domestic population. Russia did that in order to achieve surprise, weaken the legitimacy of the government, deny its involvement in attack phase, and support its legitimacy claim over the occupied territories.[149]

According to Racz`s phasing structure, the Russian objective in the preparation phase is to shape the operation environment favorable for attack by instruments of traditional foreign policy. The achieved operation environment provided a position for

[149] Racz, 67-69.

the aggressor that enabled fundamental surprise over the weakened Ukraine. Because of "the long common history, the tight economic and social ties between the two countries, as well as the strong connections between political, economic and security elites"[150] the identification of vulnerabilities was easy. Therefore, Russia was able to pinpoint those politicians, administrative officials and armed forces officers that Russia could bribe and then turned them over. The aggressor was also able to establish connection to local oligarchs, business people, local organized crime groups and separatist movements. These connections facilitated the reduction of control of central government. Simultaneously, Russia launched an aggressive influence campaign targeting Ukraine`s domestic and international audience, thus decreasing the legitimacy of the targeted government. To realize information supremacy in Ukraine, Russia established strong media positions in order to influence the local audience. Disinformation actions enabled the mobilization and preposition of regular forces on the international border, under the pretext of military exercises. The aggressor was able to achieve these objectives without crossing political or legal thresholds that would make the target country take serious, active countermeasures.[151]

The Attack phase information operation further supported the Russian endeavor to reduce the Ukraine government`s legitimacy. Organized massive anti-government protests and riots, occupied governmental buildings, sabotage attacks, blocking the central power's media, establishing communication and information monopoly in the

[150] Ibid., 58.

[151] Ibid., 58-59.

occupied territory further weakened the position of legitimate government. By establishing an alternate political power, and by denial of active Russian involvement, Russia wanted to legitimate its claim over the occupied territory towards domestic Ukraine and the international community.[152]

Russian committed a successful offensive against the Ukraine Informational power not just on the human but on the cyber terrain as well. Russia put great emphasis on cyber and electronic warfare in order to gain informational superiority over the targeted country. The well-coordinated information offensive involved not only the traditional media but also internet trolls that enabled Russia to confuse and mislead the Ukrainian and Western public.[153] Simultaneous electronic warfare and cyber-attacks can cause electronic knockdown, which paralyze the command and control system of the military and disable the administration system.[154]

The Informational instrument of national power played a vital role in the success of Russian operation in Ukraine. In the preparatory and attack phases Russia applied several informational tools to discredit the legitimacy of the government, and recruit followers to enable Russian endeavors. Regarding Informational matters, Racz identified the following prerequisites or reasons of effectiveness: elements of surprise, denial of formal involvement, weak legitimacy of the government, strong media, dissatisfied people and the attackers not being distinguishable from civilians. The existence of a

[152] Ibid., 63.

[153] Ibid., 52.

[154] Ibid., 39.

Russian ethnic minority in contested territories was a source of the legitimacy claim and was a critical factor in influencing the target audience to support Russian interest.[155] In the following section, the literature review will introduce U.S. informational concerns in UW operations.

U.S. Unconventional Warfare

The writer will inspect Military Information Support Operations (MISO) and Civil Affairs Operations (CAO), as U.S. SOF core activities, how the UW environment applies these operations, and enables the legitimacy of a supported government. The literature review will examine these core activities and identify how they affect the Informational instrument of national power, from the perspective of an aggressor country.

UW is a component part of IW and has the same general objective: fighting for the legitimacy of a supported government and for influence over the relevant population.[156] In UW operations, SOF use MISO to influence local people and the international community to support the favored government and discredit a hostile administration. "MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[157] MISO play a crucial role in the preparatory phase of UW operation, shaping the environment favorable for further operation by recruiting followers and

[155] Racz, 69-82.

[156] Joint Chiefs of Staff, JP 3-05, II-1.

[157] Ibid., II-14.

weakening the opposing government is impact on citizenry[158] MISO continue to address these shaping effects in follow-on phases as well. JP 3-05 underlines that in order to create psychological effect MISO must be integrated and synchronized with other information activities, actions of higher headquarters, and interagency partners.[159]

CAO is another SOF capability to enhance the supported government and establish supportive connections to indigenous populations. CAO identify and mitigate underlying causes of instability within civil society and enable the supported government to work effectively. CAO coordinate and synchronize activities among other government agencies, inter-governmental organizations, non-governmental organizations, indigenous population and institutions, and the private sector. Civil Affairs core tasks include: populace and resources control; foreign humanitarian assistance, nation assistance, support to civil administrations, and civil information management.[160] CAO are presented in every phase of UW operations in order to continuously enable functioning of the protected civil administration and enhance transitioning the power.[161] From the perspective of an aggressor, an adversary can use CAO in occupied territories to consolidate gains, establish collaborating governmental organizations, map the human terrain, and maintain critical services in order to acquire indigenous population support.

---

[158] Headquarters, Department of the Army, FM 3-05.130, 6-01.

[159] Joint Chiefs of Staff, JP 3-05, II-14.

[160] Ibid., II-16.

[161] Headquarters, Department of the Army, FM 3-05.130, 7-01 - 7-06.

US SOF concentrate on MISO and CAO to gain and maintain indigenous support during UW operations and to increase the legitimacy of the supported government in the targeted country and abroad. Both MISO and CAO are integrated in an interagency effort and presented in all phases of UW mission. The Russian and U.S. UW perspective offers understanding of the great powers` objectives in information matters. The following part will depict the NATO standpoint regarding countering these threats.

NATO

NATO examined the role of the human network and the significance of dynamic access to information in Strategic Foresight Analyses (SFA) in order to describe the threats of the future. According to Reed, human network is a "broad term used to describe the intricate web of relations existing in an organization and within a specific region."[162] Gomez used a technological centric approach to define the human network: "a social structure composed of individuals, business partners, friends or other organizations connected through technology, and social media, using devices such as PCs, cell phones, and PDAs."[163] The key take away from these two definitions is that even a small nation possesses an intricate web of individuals, connected to each other for specific objectives, through advanced technological means. These technological based interpersonal relations move away from the influence of the nation state. If the state loses its connection with

[162] Tristan Reed, "Intelligence and Human Networks", *Stratfor*, January 10, 2013, accessed March 11, 2017, https://www.stratfor.com/weekly/intelligence-and-human-networks.

[163] Ayana Gomez, "Human Networking," Septembeer 11, 2015, accessed January 29, 2017, https://prezi.com/j-hh_9kpe5ag/human-networking/.

individuals, it will lead to decentralization, hence to a fractured national identity. The loss of civilians` dynamic access to information, urbanization, migration, radicalization, aging nations, and loss of government monopolies over advanced technology are other potential vulnerabilities that the aggressor in hybrid warfare can take advantage of.[164] In other words, nation states have to reduce vulnerability caused by the human network, and regain some control over the population by finding areas where the state can rebuild connections.

Cederberg and Eronen find that although information related operations are gaining more and more ground on the cyber domain, the human and physical terrain remained significant. Their recommendation against the hybrid threat offers "some information still needs to be collected from human sources and classified systems. Furthermore, intelligence operators can engage in active measures within the target country, such as corrupting key officials or damaging infrastructure."[165] The two authors emphasized that information collection, physical destruction and influencing capabilities have to exist on traditional grounds, simultaneously with the modern abilities of cyber domain.

NATO Summits in Wales and Warsaw emphasized the importance of cyber defense as a crucial capability of the international security environment against hybrid threats. NATO expressed the cyber-attacks are inherent in hybrid warfare, and can be

[164] NATO ACT, "Strategic Foresight Analysis 2015 Update Report," 12-17.

[165] Cederberg and Eronen.

conducted by state and non-state actors in the context of military operations.[166] NATO designated objectives in cyber warfare such as increasing protection of NATO networks, establishing effective individual states' cyber defense measures, implementing cyber education and training, sharing information, mutually assisting in cyber resilience, and cooperating with industry.[167] These objectives connected to the protection of the command and control network, the importance of information sharing between members and the private sector, and emphasized the responsibilities of Allies. Next to the cyber defence, a well-functioning intelligence system is also a key element preventing the Alliance from the fundamental surprise of hybrid threat.

Joint Intelligence Surveillance and Reconnaissance (JISR) is vital to enable military operations, mainly in hybrid environment, where the decision makers require timely and accurate information despite the aggressor`s intensified deception activities. JISR offers a system that does not just collect information from different platforms, but allows individual nations to share information in order to facilitate a better and more timely understanding of the operational environment.[168] Joint Intelligence Surveillance and Reconnaissance still plays an important role in the fight against hybrid warfare; however, the focus of information gathering has changed and extended. The indicators of hybrid threat are not clear, and the aggressor makes every effort to hide them. In the Ukrainian crisis, Russia was able to conceal its intent until the annexation of the Crimea.

[166] NATO, "NATO Summit Guide Warsaw 2016," 124.

[167] Ibid.

[168] Ibid., 100.

The preparatory phase of hybrid warfare did not differ from the traditional measures of Russian foreign policy; hence identifying the imminent threat was almost impossible. In the Ukraine case, Russia also applied successful military deception operations, such as radio silence, hidden movement of troops, “little green men” and proxies, and imitated training exercises to cover her real intent.[169] NATO has already refocused its information collection capabilities, in order to reduce further fundamental surprise, but these capabilities have to be interconnected and augmented with other Allies and agencies.[170]

Cyber defense has become a determinative element of the Informational domain, because it is an economical and low risk method to weaken the targeted country`s Diplomatic, Economic or Military capacity.[171] Beyond financial losses, every successful attack can reduce the government`s prestige and its legitimacy, therefore making the state more vulnerable to further hybrid attacks. NATO revised and augmented its information gathering potential and established the JISR capability to connect diverse ISR platforms and facilitate timely decisions.

Influence Warfare and Weaponized Information

The author will introduce two approaches that highlight the significance of hostile influencing threats through the Informational instrument of national power. First, Patrick Tucker, the technology editor for *Defense One,* collected a variety of social science,

---

[169] Racz, 68.

[170] NATO, “NATO Summit Guide Warsaw 2016,” 101.

[171] INFOSEC Institute, “Cyber Warfare and Cyber Weapons, a Real Growing Threat,” January 15, 2015, accessed March 16, 2017, http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/#gref.

cognitive science, and psychological warfare researchers' points of view about so-called influence warfare. His study pinpointed the importance of emotion over rational facts in messages. Second, Edward Lucas and Ben Nimmo on behalf of the Center for European Policy Analysis examined Russian information warfare and observed the effect of weaponized information.

Tucker studied influence warfare and identified that the emotions are stronger than facts, in changing people`s opinions and perception. He sees Influence Warfare as a component of Information domain, which concentrates intended effects on the targeted audience. During a meeting in the Pentagon, 9 November 2016, various researchers identified and discussed the latest trend in influence warfare. "A key theme emerged: when pitching a story to an audience, emotional appeals usually beat rational dialogue."[172] Fake news and hate speech easily can affect emotions of individual citizens, while rational facts are too weak to confute them. Real democracies will be at a disadvantage to deal with state-directed hostile propaganda because they do not want to sacrifice the citizens` trust with false information. However, hostile state and non-state actors can operate with fake news, stolen emails, twitter and troll bots, etc. at low cost and low risk in order to affect people`s emotions. The targeted country also can utilize instruments to influence emotions instead of using rational dialog.[173] Although, Lucas and Nimmo utilized another approach influencing target audiences, their study further examined how the targeted country can fight against hostile propaganda.

[172] Tucker.

[173] Ibid.

Edward Lucas and Ben Nimmo identified uncertainty as a primary means of Russian propaganda and the importance of counternarrative in protecting one`s own population against hostile influence. The authors used the "weaponized information" term to depict the primary means of informational warfare. They used the words of Peter Pomeranzev and Michael Weiss to define the term: "modern Russia has weaponized information, turning the media into an arm of state power projection." For better understanding, the authors cited the motto of RT, the Russian state-owned TV channel: "Question more" because "Russian disinformation does not aim to provide answers, but to provoke doubt, disagreement and, ultimately, paralysis."[174] In other words, in influence warfare, it is not necessary to seek detailed answers or facts to support them – the projected uncertainty is enough to confuse people. Ben Nimmo characterized the application tactic of weaponized information as: Dismiss the critic; Distort the facts; Distract from the main issue; and Dismay the audience.[175] These characteristics support the findings of Trucker, because they also emphasize the strength of emotions over facts.

While seeking response to weaponized information, the authors mentioned the techniques of Hollywood and advertising-areas where the West has an advantage – in order to effect emotions. Lucas and Nimmo cautioned using the same methods to manipulate emotions and erode critical thinking as dangerous, making the West similar to

[174] Edward Lucas and Ben Nimmo, "Information Warfare: What Is It and How to Win It?," CEPA, November 2015, accessed February 12, 2017, http://cepa.org/sites/default/files/Infowar%20Report.pdf, 4.

[175] Ibid., 8.

Russia.[176] However, the counternarrative can be a more sophisticated solution against weaponized information. The aggressor builds up its influence warfare in narratives – a line of stories – "an explanation of events in line with an ideology, theory or belief" and these stories "make sense of the world" and "put things in their place according to our experience and then tell us what to do."[177] Therefore, narratives can affect people`s emotions, beliefs and their deeds.

Russia used narrative to influence the Russian ethnic minority in Estonia thus weakening the central government legitimacy. Estonia possesses the largest Russian-speaking ethnic minority in the Baltic; therefore, the literature review will examine the Estonian approach to mitigate this vulnerability.

Individual States

Russia applied the Informational instrument of national power to influence Estonian citizenry in order to ignite passions and break social cohesion between the state and people. Russia identified the Russian speaker minority in Estonia as a potential vulnerability for influence warfare. Estonia has approximately a 24.6 percent Russian-speaking population; furthermore, one third of them are Russian citizens.[178] Maigre cited Juhan Kivirähk, a leading Estonian sociologist in his Policy Brief: "the aim of Russia's

[176] Ibid., 12.

[177] Ibid., 13.

[178] Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO," The German Marshall Fund of the United State, February 12, 2015, accessed February 12, 2017, http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato, 6.

efforts to consolidate the Russian-speaking population in Estonia is not to make them a part of Estonian society, but rather to push them outside of society and to lead them into confrontation with it."[179] In other words, Russia intends weakening the central government in Estonia by dividing the ethnics in order to create vulnerability. Russia primarily uses its state owned TV channels to broadcast information across the border thus influencing Russian ethnics against the Estonian (and Latvian) government. The aggressor easily can find or create grievances that deepen the gap between the targeted audience and the government.[180] However, the Estonian government has limited and uneconomical instruments to counter the hostile propaganda.

Maigre specified that the stronger social cohesion and the values of liberal democracy are critical to overcome the Russian influential offensive, thus reducing vulnerability against hybrid threat. In order to strengthen social cohesion, Estonia intends to integrate the Russian minority. The government can facilitate integration by making it easier for Russians to gain Estonian citizenship; broadcasting trustworthy Russian language TV channels from Estonia; providing better livelihoods than in Russia; providing neutral information and better analysis at the national level and more transparent and trustworthy politicians. However, Maigre emphasized, "The small minority of Russian speakers with low incomes remains exposed to a targeted campaign by Moscow to manufacture or exploit grievances in order to divide the society."[181]

---

[179] Ibid.

[180] Ibid.

[181] Ibid., 7.

Estonia has to work out other countermeasures to control this threat and has to be aware of this minority`s potential and agenda. The aggressor in hybrid warfare will seek to multiply vulnerabilities to attack. In the Estonian example, the computer networks were the other significant weakness for exploitation.

Russia committed a heavy cyber-attack against Estonia in 2007 in order to force its government to change its policies favorably for the aggressor.[182] Estonia had vulnerability on this terrain because the functioning of the state, media, and banking websites were dependent on computer networks. The Russian state-sponsored hacker groups conducted a sophisticated and synchronized cyber-attack against the country to interrupt critical services, thereby disrupting and destabilizing the society.[183] Hybrid warfare can utilize different influence measures in order to manipulate the public opinion, even to effect indirectly on presidential elections. Germany found a different weakness on the cyber domain recently, and intends to apply a mechanism to prevent the spread of false news and hate speech, which can influence the result of the German election.

Germany was concerned about Russian influence on its domestic audience therefore co-operated with social media providers to reduce the effect of hostile propaganda.[184] The Russian government led hacker attacks on U.S. citizens and institutions indirectly affected the U.S. presidential election. The deliberate Russian

---

[182] Praks, 3.

[183] Ibid., 5-6.

[184] Amar Toor, "Facebook Rolls Out Fake News Filter in Germany," The Verge, January 15, 2017, accessed January 30, 2017, http://www.theverge.com/2017/1/15/14277964/facebook-fake-news-filter-germany.

offense against private networks resulted in a large amount of information, which influenced voters. This is not the kind of cyber war imagined in the past, but another that has crossed influence operations with espionage. Germany and other European countries worry about the Russian influence on their election in 2017. Through espionage, the aggressor can manipulate information to divide and disarray people and perhaps support the aggressor's preferred candidate.[185]

The German response seeks to eliminate or mitigate the effect of a Russian influence operation before and during the election. The German government, in collaboration with social media providers, established the "Corrective" non-profit news organization in Berlin to highlight false information spread through the internet. Individual users, supported by the fact-checking program, can mark fake news, than the "Corrective" will warn other users before they share the black propaganda. This initiative is not a government directed censorship, but involves individuals and the private sector.[186] Countering fake news and hate speech is another significant opportunity for resilience, where the population can contribute in order to reduce the effect of the aggressor`s influence warfare.

The Russian-speaking minority in Estonia provided an example of how an aggressor can use social stress to its advantage. Estonia was able to identify its weakness against influence warfare, and spent time and resources to establish counternarratives by

[185] P. W. Singer, "How Can America Beat Russia in Cyber War, Despite Trump," Wired, January 14, 2017, accessed January 30, 2017, https://www.wired.com/2017/01/america-can-beat-russia-cyber-war-despite-trump/.

[186] Toor.

mass media. However, there can be other vulnerabilities in the cyber domain that an adversary is able to utilize in order to reduce social cohesion in a targeted country. The German case introduced a solution in which a nation can involve the population to find and mark suspected weaponized information such as fake news and hate speeches, by giving the population clear understanding. The next section introduces how Russia is influencing Hungary through Information warfare.

Hungary

In his policy brief, Barabas analyzed the effect of Russian Information Warfare on Hungary, as a part of hybrid warfare. He underlined the importance of Information Warfare as a main type of effort that prepares the way for military actions by spreading propaganda or disinformation to manipulate the targeted country and the public. Because of recent elementary changes in the region in the last decade, Hungary became a battleground of informational warfare. Barabas identified these changes as the resurrection of Russian political ambitions; clashes of U.S. and Russian interest in energy and security; many-folded crisis in EU; emergence of migration; and turbulences in regional political relations.[187] These factors affect the nation`s entire DIME structure simultaneously and makes countering the threat difficult. The following paragraphs will examine how the Information Warfare targeting the population, hence weakening the position of the government and the cohesion inside the NATO and EU.

The Policy Brief highlighted the emerging trend of Russian Information Warfare in the region and its rising effectiveness to influence adversaries and cause

[187] Barabas, 3.

disorganization by confusing reality with fiction and facts with opinions. Although Russia utilizes less traditional media in Hungary, Hungarians have access to more than 100 Russian state-sponsored news and social sites, with hundreds of bloggers on the internet.[188] Therefore, the several existing Russian-inspired websites have an indirect, yet important, impact on the security risk in Hungary.[189] Barabas emphasized that Cyber Warfare is also present in Hungary and the pro-Russian Ukraine hacker group is well-known in the country.[190]

The Russian influence exists in Hungarian politics as well, where the second largest party has a pro-Russian stance. Furthermore, one member of the party in the European Parliament is under investigation for conducting espionage for Russia.[191] Most of the Russian Informational Warfare campaigns are targeting the nation`s dependence on energy imports from Russia. Through energy dependence, the Kremlin is seeking to create disunity in NATO and EU by negotiating with countries individually.[192] Barabas referred to a poll result, from 2016 by the Hungarian Nezopont Institute that 48 percent of the population accepted Vladimir Putin.[193] The writer did not seek a connection between the popularity of Putin and the Russian Informational Warfare on Hungary. The policy

[188] Ibid., 5-7.

[189] Ibid., 7.

[190] Ibid., 8.

[191] Ibid., 5-7.

[192] Ibid., 6.

[193] Ibid., 8.

brief underscored Russian propaganda in Romania, where Russian-backed Romanian sites disseminated anti-Hungarian disinformation. These messages, like "Hungary prepares war against Romania"[194] targeted the Romanian public in order to destabilize the connection between the two NATO and EU members.

Barabas examined existing Hungarian countermeasures against Russian Informational Warfare thus the propaganda and provocation to reduce tensions in Hungarian society. Budapest participates in different international initiatives, such as the NATO Strategic Communications Centre of Excellence in Latvia, fighting against a Russian media campaign. Hungary also participates in the EU`s battle against Russian disinformation in Brussels, which is a unit of public relation and communication experts to fact-check and counter the output of Russian state media. The establishment of the Cyber-defence Institute, under the Ministry of Interior was also a significant step against hostile Informational attack. Barabas did not determine the level of Hungarian participation in these initiatives, or their level of effectiveness. The protection of civilians on cyber domain is crucial for Hungary, because the internet and social media reach the majority of the population. The Hungarian Central Statistical Office reported that 79.3 percent of the population frequently used the internet in 2016.[195] The Statista statistics

[194] Ibid.

[195] Hungarian Central Statistical Office, KSH, "The Proportion of Internet Users within the Population," Hungarian Central Statistical Office, accessed March 29, 2017, http://www.ksh.hu/docs/eng/xstadat/xstadat_annual/i_oni016.html.

portal projected 5 million social media users in Hungary in 2017, which is more than 50 percent[196] of the 9.8 million citizens.

Regarding the Informational instrument of national power, the literature review inspected the crucial role of information in hybrid warfare through the Ukraine conflict and from the view of U.S. UW. The review identified that the information collection, influence warfare and information protection exist in all phases of the hybrid aggression and aimed the legitimacy of the targeted government through the population`s perception. Concerning the Ukraine case, Racz highlighted several reasons for effectiveness: elements of surprise, denial of formal involvement, weak legitimacy of the government, strong media, dissatisfied people and the attackers not being distinguishable from civilians. The U.S. UW approach underlined the integrated nature of MISO and CAO, thus the necessity of cooperation between interagency, inter-governmental and non-governmental organizations. While MISO concentrate on gaining and maintaining indigenous support and increasing the legitimacy of the supported government, CAO are able to increase the effectiveness of the government in the controlled territories.

NATO emphasized the importance of cyber-defense and JISR capability in the fight against hybrid warfare. While the significance of cyber domain is increasing, traditional terrains are remaining crucial as well. The human terrain is highly vulnerable against sophisticated influence warfare operation or weaponized information. Estonia and Germany provided examples for how individual states can take countermeasures against

[196] Statista, "Forecast of Social Network User Numbers in Hungary from 2014 to 2021," accessed March 29, 2017, https://www.statista.com/statistics/568952/predicted-number-of-social-network-users-in-hungary/.

cyber-attack or influence warfare. Hungary also suffers Information Warfare attacks from Russia, which affect the public opinion, economy, and diplomacy fields, even intending to weaken connections with other NATO and EU Allies. The next part of the review will examine those literatures, which deal with society involvement in a national defence strategy, thus with the correlation between Military and Information instruments of the national power.

Correlation between Military and Information Power

In order to find recent applications that enable interactions between the Military and Informational instruments of national power, the literature review will examine those scholars that connected the state`s defense strategy with citizenry`s involvement, thus influencing civilians to take part in military activities. First, Racz`s study will explain the role of proxies in the Ukraine conflict, and how Russia facilitate a discord between the government and population. Second, the author will examine U.S. UW and how it utilizes MISO to gain indigenous support for resistance movement while decrease the adversary`s defense capability. Third, the review will inspect NATO`s resilience recommendation in detail, concentrating on civil preparedness in defensive matters. Fourth, the writer will present the perspective of small states, describing the potentials of territorial defense forces and resistance movement for connecting the people and the state. Finally, the Hungarian standpoint will be introduce on the society involvement in the nation`s defence.

Russian Aggression against Ukraine

According to Racz, Russia utilized information power to influence Russian sympathizers, organized crime groups and corrupt Ukraine officials fighting against the Ukraine government. Furthermore, the aggressor used propaganda to decrease the Government legitimacy, to reduce morale, to isolate military leaders from sources of information and for military deception.[197] The Russian proxy force consisted of local separatists, oligarchs, business people, organized crime groups, and bribed military and non-military officers. Their role was crucial supporting the legitimacy claim of invading Russian troops, and denying Russian formal involvement.[198] Not just the weak government, but the well-organized preparation phase assisted Russia to identifying potential proxies, building up propaganda campaign via media in order to influence the target audience and weaken the Ukrainian security forces response capability.[199] In other words, the aggressor heavily concentrated on the Informational instrument to isolate citizens from the government, enroll them into proxy forces and attacks on loyal security forces, the Military instrument, through or with these separatists. The following paragraphs will describe U.S. UW operations regarding the integration of Military and Informational power.

[197] Racz, 76-77.

[198] Ibid., 69.

[199] Ibid., 58-60.

Information related operations in UW help bolster support for indigenous forces among sympathizers and the uncommitted populace.[200] The success of UW operations depends on the resistance movement, how U.S. forces can fight through or with them to overthrow a government or defeat occupying forces. As it was aforementioned, the resistance movement consists of a large segment of the population, including the supporting mass base; therefore influencing the citizenry is crucial in UW operations.

MISO enable the resistance movement with the following objectives: (1) Creating popular support for the resistance movement; (2) With this support allowing freedom of maneuver and assist avoiding detection; (3) Promoting recruitment; (4) Discrediting the government; (5) Supporting the shadow government; (6) Enabling U.S. support and presence; (7) Creating defection among enemy forces; (8) Winning the support of the uncommitted; (9) Developing unity and maintaining motivation in UW forces.[201] These objectives facilitate the establishment and augmentation of the resistance movement, but simultaneously reduce the capability of the enemy`s military and government. FM 3-05.130 underlines that these information related operations are more significant in the preparatory phase.

Legitimacy is a vital factor in UW operations, due to developing and maintaining international and internal support. U.S. law and national policy prohibits supporting

[200] Headquarters, Department of the Army, FM 3-05.130, 6-1.

[201] Ibid.

terrorists and organized elements and groups violating international law,[202] while supporting justified legitimacy claims, which promote the credibility of U.S. UW operations.[203] In order to counter the hybrid threat, NATO emphases the resilience for Allies to maintain basic functions of the government, prepare civil support for armed forces and keep up adequate military capability.

NATO

During the NATO Summit in Warsaw, the Alliance recommended resilience as a necessary capability of individual state for resisting hybrid threat. Resilience is the combination of civil preparedness and military capacity and pursues to maintain and develop individual and collective capacity to resist armed attack.[204] The civil preparedness part of resilience is inherently connected to the citizenry, and needs support from the population to enable military efforts. The Summit highlighted why civil preparedness has become important again in hybrid environment, where the commitment of conventional forces is possible.

During the Cold War, states that had control over civil resources and critical infrastructure also maintained territorial defense mechanisms ready to support war efforts. However, after the Cold War, the private sector owned, operated and controlled key resources and infrastructure and reduced redundancies to further increase profits. According to NATO estimates in large-scale operations, 75 percent of required host

[202] Ibid., 3-18.

[203] Ibid., 4-3.

[204] NATO, "NATO Summit Guide Warsaw 2016," 131.

nation support, 50 percent of satellite communication and 90 percent of military transport is sourced from commercial infrastructure and services.[205] Through civil preparedness, thus with active cooperation between government and the private sector, NATO and its members want to regain essential control over these crucial and vulnerable capacities in order to enable large-scale conventional operations in supported countries.[206]

In order to satisfy the resilience requirement, nations have to maintain basic government functions, and have to involve and prepare the civil sector to maintain services in case of hostilities. Under Article 3 of NATO, all Allies are committed to building resilience, therefore civil preparedness to support domestic and NATO forces, and military capacity to defend the state until NATO forces arrive or to enable Article 5, collective defense missions.[207] Territorial Defense Forces are suitable possibilities to build military capacity in order to defend the nation`s integrity as long as NATO forces intervene in the conflict under collective defense obligation.

Territorial Defence Forces

Individual states in NATO utilize Territorial Defense Forces (TDF) to augment their standing regular armed forces capability with a regular, territorial based reserve force in order to strengthen defensive capacity, deter adversary and to involve “civil

[205] Ibid., 132.

[206] Ibid., 134.

[207] Ibid.

society in protecting the country."[208] Baltic and Nordic countries, as well as Poland view TDF as one of the elements in their national defence systems' response during the early stages of a hybrid conflict, organized on territorial base. Volunteer or compulsory troops can serve in these formations.[209] The following paragraphs will examine why Estonia, Latvia and Lithuania want to develop TDF and encourage citizens to serve in these formations.

Szymanski used the Swedish model to introduce TDF, which are organized into units corresponding to the state administrative divisions. TDF can participate in search and rescue, crisis response, border monitoring, guarding lines of communication, protecting facilities, and reconnaissance tasks in peacetime. In wartime, TDF can conduct targeting, as well as defending critical infrastructure. Because members of the TDF are recruited from local communities, they are familiar with the assigned area. The writer underlines that TDF have little chance of prevailing against conventional or SOF aggression, but are able to neutralize armed civilian groups and riots, strengthen the security of infrastructure, and support friendly UW operations in lost territory.[210] Baltic states utilized the Swedish model with different applications.

Estonia maintained conscription as the foundation of its defense strategy, but with a professional component and with the volunteer Estonian Defense League. The Estonian

---

[208] Olevs Nikers, "Inside Latvia's New Defence Strategy - Riga Declares Its Military Ambitions," LRT, June 7, 2016, accessed March 21, 2017, http://www.lrt.lt/en/news_in_english/29/139072/inside_latvia_s_new_defence_strategy_riga_declares_its_military_ambitions

[209] Szymanski.

[210] Ibid.

TDF have their traditional functions complementing anti-tank warfare capability. The country wants to keep its conscription system and increase TDF capacity by developing the firepower, strength, and training as well as equipping the reserves with the same equipment as the professional forces. In order to shorten the readiness time of TDF by 75 percent, Estonia fielded firearms and ammunition to reserve service members.[211] Although the Estonian Defence Forces are based on conscription and they have applied the principle of total defense, they also possess a voluntary component, the Defense League that increases the national defense potential and directly involves citizenry in military matters.

The Estonian Defence League provides more than 20,000 regular soldiers to augment the active and conscripted reserve forces. The Defense League consists of male and female soldiers and educates youngsters in patriotism and defending national sovereignty.[212] This number of soldiers is a noteworthy augmentation of the professional force and establishes a direct connection between soldiers and civilians.

Estonia developed its cyber defense capability by establishing the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn.[213] This endeavor promotes the nation`s capacity against further cyber-attacks. The Defense League also encompasses a Cyber-Defense Unit – volunteer professionals recruited from the private

---

[211] Ibid.

[212] Riigi Teataja, "The Estonian Defence League Act," February 28, 2013, accessed December 2, 2016, https://www.riigiteataja.ee/en/eli/525112013006/consolide.

[213] NATO, "NATO Summit Guide Warsaw 2016," 126.

sector. The objective of this unit is to "identify and develop forms of collaboration and communication among the various stakeholders involved" and "raising public awareness on cyber threats and cyber security."[214] In other words, the Cyber Defence Unit promotes the connection between the professional in private sector, the citizenry, the military, and governmental agencies. The other two Baltic states utilize similar methods in order to protect their sovereignty against the Russian hybrid threat.

Latvia and Lithuania abolished conscription and introduced professional armed forces model in 2008, so their TDF was based on a volunteer system and serves as reserve forces on territorial base. The Latvian National Guard performs anti-tank, anti-aircraft tasks, countering weapons of mass destruction, and conducts engineering work. In Lithuania, the National Defence Volunteer Forces organized as a TDF performs tasks related to anti-tank and urban operations. Additionally, Lithuania has another volunteer organization, which prepares young people to join to the National Defence Volunteer Forces later on. In both countries, Ministries of Defence increases spending on TDF matters in order to provide better equipment, training, readiness capability, and integration with professional forces. Demographic crises affect the manning of TDF, so there are not enough volunteers to fill vacant position in armed forces. After the annexation of Crimea, public interest increased and more citizens signed for professional or paramilitary forces, but the imminent threat from Russia reduced willingness to join

[214] Kadri Kaska, Anna-Maria Osula and LTC Jan Stinissen, "The Cyber Defence Unit of the Estonian Defence League," 2013, accessed February 20, 2017, https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf, 7.

the reserve or active formations.[215] Both states were about to reintroduce compulsory conscription, but in Latvia, political and financial considerations delay the decision.[216] Lithuania`s State Defence Council finally decided to reintroduce the mandatory military service in 2015 in order to raise recruitment number to 3,500-4,000. However, in 2016 two thirds of the recruits came forward voluntarily.[217] The next paragraph examines the main tasks of TDF in the three Baltic states.

Baltic states invest in youth organizations affiliated with TDF to increase the spirit of pro-state values, including the Russian-speaking minority participation in TDF. Beyond those tasks that were listed before, all states utilize TDF for the following missions: cyber-defense, public defense education, and host nation support for incoming NATO troops. The Estonian TDF also prepares for sabotage and guerilla warfare[218] a significantly different UW characteristic compared with general conventional nature of TDF in the Baltic region.

Russia has recognized the importance of TDF as well, but is struggling with several problems in order to make it effective. Kaufman, a research scientist at the Center of Naval Analysis, highlighted problems that the Russian TDF have faced since the reestablishment of territorial reserve formations. Between 2008 and 2012, Russia only

---

[215] Szymanski.

[216] Nikers.

[217] The Baltic Times, "Lithuania to Reintroduce Permanent Conscription," *The Baltic Times,* March 15, 2016, accessed April 18, 2017, http://www.baltictimes.com /lithuania_to_reintroduce_permanent_conscription/.

[218] Szymanski.

has a list of people and a list of equipment as reserve capacity without training, therefore without any real capability to enable active duty forces during conventional conflict. Although that time, the Russian reserve forces were able to work for basic territorial defense units, guarding checkpoints or facilities, but they were not able to conduct combat operations and did not possess adequate mobilization ability. Putin realized this vulnerability and issued orders to rebuild the reserve forces on a TDF base. The experimental pilot program involved 5,000 reservists and lasted from 2012 to 2016, and finally produced territorial defence battalions with an adequate mobilization system, command staff and equipment. This amount of TDF is definitely not enough to support active duty forces in large-scale combat operations, but can be a good basis to develop more troops. Regardless of special emphasis on the importance of TDF from Putin, the four-year effort, the huge amount of allocated funds, and the undergoing Ukrainian crises, Russia was able to introduce TDF with only 5,000 manpower.[219]

Resistance Movement

Baltic states are exploring the possibility of applying the resistance movement as part of armed capacity of resilience to fight against hybrid threat. U.S. Special Operations Command Europe sponsored and led Resistance Seminar Series and is looking for adaptable solutions for response. The seminar emphasized “preparatory requirements that

[219] Michael Kofman, “Russia’s Territorial Defense Battalions Are Finally Here,” Russian Military Analysis, September 2, 2016, accessed March 21, 2017, https://russianmilitaryanalysis.wordpress.com/2016/09/02/russias-territorial-defense-battalions-are-finally-here-all-two-of-them/.

are necessary to set the conditions for any resistance activity that may be required."[220] The conference divided the timeline of the hybrid war into two periods. The first period is before the attacked country loses its sovereignty, the armed segment of resilience dominates, and provides deterrence capability to defend the nation`s integrity. This period also consists of preparation efforts setting conditions for second period`s irregular warfare, simultaneously strengthening the overall resilience capability, thus increasing the deterrence capacity. The second period starts when a country loses any of its territory, the resistance movement can facilitate regular formations to regain sovereignty.[221]

Other observations of the Baltic Seminar Series underline the importance of national level narratives as a part of the Informational instrument of the nation power, which "promote national cohesion and foster unity of effort."[222] Different periods of counter hybrid warfare require different approaches in information operations, but have to cover internal and external audiences including the adversary's population. In the preparation-deterrence period, the targeted country has to use legitimate and credible messengers in order to promote citizens' situational awareness and establish narratives against potential informational vulnerabilities. In the resistance period when the nation loses territorial integrity, information operations must focus on ensuring "the legitimacy and credibility of the government."[223]

---

[220] The National Academy of Defence of the Republic of Latvia, 3.

[221] Ibid.

[222] Ibid., 4.

[223] Ibid.

The seminar finally underlined the significance of pre-crisis preparation activities that enable basic governmental functions and services during open armed conflict, when centralized control diminishes.[224] The institutional collaboration must support the resilience endeavor with the unity of effort between "government ministries, civic organizations, and the larger public."[225]

Participants in the Resistance Seminar Series worked out an irregular warfare centric defense strategy against a hybrid threat. This method can facilitate the NATO Warsaw Summit resilience endeavor by building an armed deterrence segment, as well as civil preparedness. Domestic preparation for unconventional warfare, supported by a broad spectrum of information operations, interagency, inter-governmental efforts and the integration of other various stakeholders` efforts, can facilitate close interaction between Military and Informational powers and promote cohesion in the society. Not only armed resistance movement can support the nation`s defense capability, but nonviolent resistance is able to promote this endeavor as well.

Bartkowski argued that nonviolent civil resistance could also be an effective measure against hybrid threat. The nation can wage a long-term, all-encompassing and targeted noncooperation effort against the aggressor to disrupt its control and undermine its legitimacy.[226] While he underlines the importance of armed deterrence by NATO

---

[224] Ibid., 5.

[225] Ibid., 6.

[226] Maciej Bartkowski, "Countering Hybrid War: Civil Resistance as a National Defence Strategy," Open democracy, May 12, 2015, accessed March 23, 2017, https://www.opendemocracy.net/civilresistance/maciej-bartkowski/countering-hybrid-war-civil-resistance-as-national-defence-strateg.

prepositioned forces or by paramilitary groups in armed resistance, Bartkowski argued that the nonviolent resistance has more support from the population and its significance is higher than is often recognized. He referred to the Russian military doctrine, released in 2014, that social movement and civil-led demonstration are major weapons in territorial conflicts, as it was observed in the Color Revolutions or at the Ukrainian Euromaidan. Nonviolent resistance is especially relevant to smaller nations, because they are more vulnerable to hybrid threats, and the aggressor is eager to manipulate their population. Historically, civilian resistance is twice as effective as armed struggle, can mobilize eleven times more mass than armed resistance and is likely to reduce civilian deaths.[227] Conscious preparation for nonviolent resistance can widen the opportunities against hybrid aggression by involving citizenry to realize an advantage on Informational and Military instruments of the nation`s power. The next part will present Hungarian literature on this topic.

Hungary

The Hungarian Minister of Defence, Dr. Istvan Simicsko, held a conference in November 2016, and expressed his plans about HDF development and the reconsideration of reserve forces on a TDF base. The minister underlined the necessity of strengthening relations between the HDF and society, and underlined that "nothing can substitute for nation states."[228] In other words, countries` sovereignty is still important in

[227] Ibid.

[228] Hungarian Ministry of Defence,"Relations Must Be Strengthened between the Hungarian Defense Forces and Society."

Europe, even under the pressure of new security challenges. Therefore, the HDF must prepare for this contest.

The minister emphasized that according to the Hungarian Fundamental Law, the three pillars of the nation`s security are the strength of the HDF, the system of Alliance and the citizens. In order to enhance the citizens' involvement and efforts in national defense, the government intends to provide practicable military knowledge for volunteers, establish the National Defence Sports Federation, promote patriotism in the younger generation, develop shooting ranges and reach out to other non-radical self-defense organizations like the civil militia. During the congress, the establishment of territorial defence reserve forces was announced as well. Finally, the minister pointed out that these changes require an intergovernmental effort.

In February, 2017 the Minister of Defence disclosed the Zrinyi 2026 development program, which intends to increase the capability of active armed forces, the military communication and information system and cyber-defence. However, the program also envisions the development of reserve forces in order to extend the currently 5,300 volunteers, and reorganize them on territorial basis.[229] Further details are not available on the territorial defense reserve forces, due to ongoing elaboration.

Hungary recognizes the importance of the involvement of citizenry in the defense strategy, furthermore has the willingness to invest in this endeavor. The Zrinyi 2026 development program intends to improve the capability of the active armed forces to

[229] MTI, "The Hungarian Defence Forces Must Be Made a Major Military Force in the Region by 2026," Website of The Hungarian Government, February 16, 2017, accessed March 24, 2017, http://www.kormany.hu/en/ministry-of-defence/news/the-hungarian-defence-forces-must-be-made-a-major-military-force-in-the-region-by-2026.

achieve the requirements of NATO standards, but also revises the existing reservist system to increase citizens` participation in the nation`s defence. The following part of the literature review will examine how hybrid warfare can utilize extremist groups in Hungary to weaken social cohesion.

Sonkoly, in his Master`s Thesis, examined the threat from right-wing extremist movements that intended to overthrow the existing social order of Hungary and conducted activities with paramilitary features,[230] as a part of hybrid threat. He applied quantitative analysis to different radical groups to interpret their motivation, goals and connections to identify possible solutions to neutralize this threat. The ideologies of these movements based on national redemption, anti-Semitism, mainly against Gypsy minority, and accusations against political elite.[231] Furthermore, these groups shared negative views on the HDF, and established paramilitary self-defense organizations.[232] The thesis underlined the connection between extremist groups, the Hungarian right-wing political party and Russia. All over Europe, Pro-Russian extremist groups aimed to undermine the EU and NATO from within.[233] Russia supported these extremist organizations in order to weaken the social order in the country by influencing radical citizens.

[230] Tibor K. Sonkoly, "Aggressive Neighborhood Watch or Unconventional Threat? The Hungarian Extreme Right-Wing Self-Defense Movements" (Master`s Thesis, Naval Postgraduate School, Monterey, CA, 2014).

[231] Ibid., 9.

[232] Ibid., 10.

[233] Ibid., 14.

Sonkoly identified not just the threat in these right-wing paramilitary groups, but also the opportunity presented by this phenomenon. One of their other rhetoric, the national self-defense, is an important feature that Hungary can facilitate. He argued that the government could absorb individuals from extremist groups under an umbrella of legal organization but without radical ideology.[234] Sonkoly visualized a solution that integrate a counter-UW capability in HDF; a communication campaign to form public opinion and trigger tensions in self-defense groups; and reintegration and moderation of extreme insiders.[235]

The thesis pointed out that these volunteer self-defense groups consisted of citizens who intended to protect the nation`s territorial integrity, who even spent lots of time for military training. Volunteers have the willingness to conduct three days in training focusing on close combat, weapon drills, small unit tactics, and psychological preparation. During advance training, participants received more sophisticated skills.[236] Although these paramilitary groups, sponsored by an aggressor are very dangerous for the Hungarian democratic order, through their reintegration or moderation, the nation can gain volunteers to defend the state`s integrity.

This part of the literature review described why the integration of Military and Information instruments of national power could promote the involvement of citizenry in hybrid environment. Both the aggressor and the targeted country are seeking civilian support in order to attack or defend the legitimacy of the existing government. Russian

[234] Ibid., 63.

[235] Ibid., 70.

[236] Ibid., 17.

and U.S. literature introduce the standpoint of the occupying force, and why the establishment of indigenous assistance is crucial to fight with or through occupying forces to reduce the government`s legitimacy. NATO underscored the significance of civil preparedness, as the part of resilience, which is crucial in large-scale operations to support domestic or incoming NATO military forces. Individual states presented two different solutions regarding the augmentation of military capacity of resilience. The first was the Territorial Defence Forces that was primary conventional in nature and could build on conscription or volunteer membership. The second was the resistance movement that could be violent or non-violent, could involve more volunteers, and provide more deterrence against a hybrid aggressor. From the Hungarian perspective, the review presented the official approach of the Ministry of Defence that committed to establish a territorial based volunteer reserve force while increasing the capability of the standing active defence forces. The other approach highlighted the danger of foreign sponsored radical groups, however pointed out the opportunity of moderated and integrated self-defense associations. The next section will summarize chapter 2.

Summary and Conclusions

The second chapter provided an overall literature review about existing problems and proposed or practiced answers against hybrid warfare. The writer examined the threat through the Russian aggression in Ukraine and U.S. UW doctrines. Regarding counter hybrid warfare, the review introduced NATO`s position from the standpoint of the whole Alliance and, in parallel, examined the aspects of small individual states and presented the current situation in Hungary. The last part of the review concentrated on the

interaction between Military and Informational powers, where the author presented the most recent solutions for how a state can involve citizenry into the nation`s defense.

Regarding to the threat, the author identified the following themes:

1. The population, and the government`s legitimacy are the primary targets of hybrid warfare;
2. Through operations on informational domain the aggressor shapes the environment for military intervention;
3. The aggressor aims the entire DIME structure simultaneously;
4. The invader denies its involvement in order to confuse the international community, and to avoid international intervention;
5. During hybrid operations, the aggressor takes advantage of the difficulty identifying enemies and civilians, and the shortfalls of legal system;
6. Surprise is a decisive element, mainly in the attack phase;
7. Military superiority, disintegrated government, weak security forces, ethnic or political vulnerability, real or perceived legitimacy claim, strong media presence, and favorable terrain are important prerequisites of hybrid offence;

From the counter-hybrid warfare standpoint, the literature review consisted the following themes:

1. Reassured NATO collective defense endeavor, establishment of very high readiness task forces;
2. Prepositioning forces and command posts at NATO`s peripheries;
3. Building resilience capability with civil preparedness and military capability in individual states;

4. Significance of readiness and quick reaction capability;
5. Integrating intelligence collection, cyber-defence, and fact-checking or counter propaganda capabilities inside the Alliance;
6. Involving the society in the nation`s defence;
7. Establishing of territorial defense forces, which can be volunteer or conscripted, but focusing on conventional warfare;
8. Using traditional and non-violent resistance movements as segments of the resilience;
9. Countering hybrid threats has to be based on intergovernmental and interagency effort, with close cooperation with private sector and non-governmental organizations;
10. Protecting the population from hostile propaganda, as well as key officials and radical groups from the influence of an aggressor;
11. Gaining support and volunteers from the population;
12. Neutralizing or integrating unofficial self-defense movements;
13. Supportive legal system to commit timely and appropriate countermeasures.

The next chapter will present research methodology, and how the analysis will proceed to obtain information needed, in order to address the primary and secondary questions of the thesis.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

The purpose of this study is to generate options for the HDF decision makers regarding the Military and Informational instruments of national power in order to strengthen Hungary's resilience against hybrid warfare.

This chapter describes what kind of steps have to be taken to obtain information needed, and what kind of methodology enables the study to answer the primary and secondary research questions, and introduces applied criteria. In order to recognize areas where the correlation between Information and Military instruments can foster Hungary`s resilience capability against hybrid threats, the analysis has, first, to identify the state`s vulnerabilities. To protect these critical vulnerabilities, the analysis recommends solutions based on best practices that are adaptable in the specific contemporary Hungarian security environment.

Applied Methodology

The thesis aims to examine the current Hungarian security environment in hostile hybrid conditions and seeks possible solutions for it. Because the Hungarian "case is a specific, complex, functioning think,"[237] and the author has interests only in this unique case, the thesis applies qualitative intrinsic case study methodology to answer the primary and secondary research questions. Documents in the literature review provide two

[237] Robert E. Stake, *The Art of Case Study Research* (Thousand Oaks, CA: SAGE Publication, 1995), 2.

primary sources to identify the threat, the Ukraine-Russian conflict and U.S. UW, and several others that offer solutions countering hybrid warfare. These sources deliver opportunities for generalization, and through these findings, the analysis intends to provide particularization on the unique Hungarian case.[238]

Because the problem has an ill-structured and asymmetric nature, the analysis applies the Army Design Methodology to define the problem and to seek possible solutions.[239] Army Design Methodology offers ways through framing the operational environment by identifying current conditions, projecting possible trends and describing the desired end-state.[240] The problem statement addresses the gap between the existing security environment and the desired one. By formulating an operational approach, the author identifies the center of gravity, determines direct or indirect approaches, and lines of effort.[241] Because the literature review offered several different solutions against the hybrid threat, the analysis inspects these possibilities and recommends those that are feasible for reaching the end-state.

The author assumes that hybrid warfare with highly integrated design would be the trend in future conflicts, therefore understanding its potential effect on Hungary is vital. In order to identify possible outcomes of a hybrid attack and courses of actions of

---

[238] Ibid., 7-8.

[239] Headquarters, Department of the Army, Army Techniques Publication (ATP) 5-0.1, *Army Design Methodology* (Washington, DC: Headquarters, Department of the Army, 2015), 41.

[240] Ibid., 3-1 - 3-6.

[241] Ibid., 5-2.

the adversary, the thesis examines prerequisites and success criteria of the Russian-Ukrainian conflict and U.S. UW doctrines adapting to the current Hungarian security environment. The recent Russian – Ukrainian conflict and the extended U.S. experience in UW operations provides opportunity for generalization to identify key characteristics for how a great power can influence a small state. The analysis utilizes Political, Military, Economic, Social, Information, Infrastructure, Physical environment and Time (PMESII-PT) framework to identify the threat. These findings offer a chance to apply the general threat to the current Hungarian security situation for particularization. The outcome answers the first secondary question by identifying hybrid challenges that Hungary has to prepare for using Military and Information instruments of the nation`s power.

In order to identify possible solutions for Hungary against hybrid threat focusing on Military and Informational concerns, the thesis inspects NATO recommendations, and denouement from individual states for generalization purpose. In the literature review, some significantly different themes have emerged as solutions for the involvement of citizenry into the nation`s defense endeavor. These distinctions were regarding conscription or volunteer forces system, conventional Territorial Defence Forces or unconventional resistance movement, as well as passive and active resistance. Therefore, it is necessary to examine these different options to determine how these can complement one another. The solutions from NATO and individual states must be examined in the unique Hungarian security environment for particularization. The resulting answers on the second secondary question identify that by the interaction between Military and Information instruments of national power, how can Hungary involve its citizenry in order to realize feasible resilience capability?

The analysis identifies the potential hybrid threat against Hungary, enemy and friendly centers of gravity, and lines of effort to achieve a feasible end-state through the Russian hybrid and U.S. unconventional warfare literature. In order to define denouements, the thesis examines NATO and individual states` counter hybrid approaches to offer an adequate solution for Hungary. The following paragraphs present criteria for the analysis.

Criteria

The case study analysis concentrates on the first two phases, the preparatory and the attack of hybrid warfare according to Racz phasing structure, which concurs with the first six phases of U.S. UW concept. The assessment examines the preparatory phases to identify how an aggressor shapes the environment to initiate the attack creating the conditions that enable the second phase. The analysis explores the attack phase in which the targeted country is unable to deter the hybrid threat and has to fight. The study does not inspect the stabilization phase in detail, because it primarily employs diplomatic instruments, major military operations are terminated and the state has already lost control over its territory.[242] In the U.S. UW phasing system, the seventh, transition phase equal to the stabilization phase, where invading forces consolidate their gains, and assist to the supporting government in reconstruction.[243] The analysis will examine the DIME framework in each phase focusing on the Military and Informational domains.

[242] Racz, 57-67.

[243] Headquarters, Department of the Army, FM 3-05.130, 4-10.

In order to evaluate the threat, the analysis examines Russian aggression against Ukraine through Racz`s study, which offers a recent hybrid warfare example. Characteristics of U.S. UW are very similar to hybrid warfare as chapter 2 introduced. Both types of warfare are the instruments of a great power against a weaker one, aim to influence the population, and facilitate the victory of the supported government. The Russian hybrid and U.S. unconventional warfare synchronize the nation`s entire power in order to engage the targeted country`s DIME structure simultaneously. Furthermore, both heavily utilize information-related operations to acquire local and international support for the intervention and Special Forces to engage proxies in order to fight with or through indigenous forces. Due to these similarities, the analysis uses these two types of warfare for generalization, to find possible enemy`s Courses of Actions and outcomes of a hybrid attack. The author intends to apply these findings on the unique Hungarian situation in order to evaluate the effects of the threat, and identify critical vulnerabilities.

Emerging themes in the literature review define the desired end-state of a country under potential hybrid warfare, which is the primary criterion of the analysis. The nation-state wants to preserve her sovereignty and territorial integrity against hybrid aggression. That must be the Hungarian desired end-state as well. In order to achieve this end-state, the literature review offers the following themes[244] that become the conditions of the operational approach: retain the constitutional order and the legitimacy of the prevailing government; gain the citizenry`s commitment for the nation`s defence; prevent surprise; possess adequate military deterrence capability; possess adequate informational

[244] Themes can be found in the Summary and Conclusion section of chapter 2.

deterrence capability; enable NATO Article 5, collective defense intervention; create "whole-of-government" approach in the defense sector. The analysis process can modify these offered conditions.

In order to find appropriate solutions the analysis examines the NATO counter hybrid warfare Military and Information related endeavors, and inspects how these align with individual states` applications listed in the literature review. Each mentioned individual state has had some intimidation from Russian hybrid warfare, therefore their procedures or applications are relevant for studying countermeasures. It is not possible to evaluate which solution is right or wrong, since it is not clear that the deterrence is successful, or Russia is still shaping the operational environment for further aggression. Through the examination of the current Hungarian security situation, the author identifies friendly center of gravity, determine direct or indirect approaches, and lines of effort.

After the creation of lines of effort, the analysis identifies risks in the plan, offers mitigation measures, and emphasizes the possible effects of taking prudent risks. The process concludes in the mission narrative, which is the expression of the operational approach, summarizes the result of the conceptual planning, and informs and educates key stakeholders whose perceptions are relevant for success.[245] The next section summarizes chapter 3.

[245] Hedquarters, Department of the Army, Field Manual (FM) 5-0, *The Operations Process* (Washington, DC: Hedquarters Department of the Army, 2010), 3-11 - 3-12.

Summary and Conclusion

The research methodology introduced the structure of the analysis, and the intent to answer the primary and secondary research questions. The chapter also depicted those areas where the author concentrates and why. Finally, it described those criteria that prevent ambiguity, thus promote the credibility of the next chapter. Chapter 4 consists of the analysis of this thesis.

CHAPTER 4

ANALYSIS

Introduction

The purpose of this study is to generate options for the HDF decision makers regarding the Military and Informational instruments of national power in order to strengthen Hungary's resilience against hybrid warfare.

This chapter answers the primary and secondary research questions. Through the description of the threat, it responds to the first secondary research question, what are the hybrid challenges for which Hungary has to prepare? Then the analysis answers the other secondary research question, how can Hungary involve its citizenry in order to realize feasible resilience capability? Through the secondary research questions, the mission narrative synthesizes the response to the primary research question, how interaction between Military and Information instruments can facilitate Hungary`s resilience capacity, in order to deter adversaries, and maintain the nation`s sovereignty? Finally, chapter 4 summarizes findings during the analysis process.

The Threat

This section of the analysis provides answers to the first secondary question: what are the hybrid challenges for which Hungary has to prepare? In order to answer the problem, the thesis analyzes the Hungarian security environment from the perspective of the Ukraine-Russian conflict, regulations of UW operations, and Hungary`s current circumstances. The aggressor`s overall end-state is to exercise desired political influence over Hungary. The next section analyzes potential effects of a full-spectrum hybrid attack

on the current Hungarian security environment through PMESII-PT framework. An adversary uses hybrid warfare against Hungary applies the preparatory and transition phases as shaping, and the attack phase as decisive operation. The analysis aims to uncover how the adversary can successfully shape the environment to commit the attack phase, as well as how to realize victory to enable the stability phase. Finally, the author identifies the enemy`s course of actions that facilitates the adversary`s end-state to exercise desired political influence over Hungary.

Political

From the internal political perspective, the adversary can weaken the legitimacy of the actual government by alienating citizenry. The foe influences citizens to support radical parties, groups and movements, in attacking the constitutional and social order, or establishing government favorable to the opponent by taking advantage of the aggressor`s funding and power. The adversary explores vulnerabilities of the state administration and municipal governments by bribing politicians, in order to overthrow central authorities or decrease their effectiveness. With false news and hate speeches, the foe manipulates the population and indirectly influences elections` outcomes. In the attack phase, the opponent organizes massive anti-government protests and riots in order to disable the central power and capture administrative buildings. Finally, the foe declares an alternative political center in occupied areas.

From the external political viewpoint, the foe manipulates international audiences in order to isolate the country and prevent support from abroad. By facilitating hostility between Hungary and another NATO member, like Romania, or by influencing the population to oppose NATO membership, the aggressor can seriously damage the

Hungarian defense capacity and simultaneously discredit the Alliance. The exit from EU can cause similar outcomes in the Diplomatic and Economic instruments of national power. During the attack phase, the adversary tries to mislead and misinform the international audience to introduce the conflict as a domestic issue in order to prevent or delay NATO or United Nations intervention. Most importantly, the potential aggressor utilizes traditional measures of its foreign policy, and does not need to cross any political or legal threshold that would initiate serious, active countermeasures from Hungary. Furthermore, because of "Hungary does not consider any country as its enemy,"[246] the defense sector has no specific threat to prepare for, thus mainly concentrating on emerging problems, like NATO and United Nation deployments and the refugee crisis.

Military

The aggressor supports radical movements, creates military wings and finance, equip, train and lead them against military and key infrastructure targets. The opponent establishes contact with criminal groups and oligarchs in order to utilize them for armed attacks, smuggling supplies and combatants through national borders, and decreasing the legitimacy of security forces. The aggressor encourages immigrants to move and settle in Hungary to ignite passions among locals, migrants, and partner nations in order to cause economic problems as well as overburdening security forces. Through refugees, the adversary can infiltrate terrorist elements to decrease citizenry`s sense of security, thus the legitimacy of the government. By taking advantage of the lack of coordination between security forces, governmental agencies, along with the insufficiency of

[246] Hungarian Ministry of Defence, "Hungary`s National Defence Strategy," 5.

legislation to utilize proper force, the foe intends to maintain the hostility under the NATO Article 5 threshold. The aggressor also can prevent or divide collective defense response, by creating conditions for the commitment of NATO military readiness forces in other theaters.

In order to realize surprise in the attack phase, the aggressor bribes key stakeholders in the armed forces, paralyzes command and control systems with misinformation and electronic warfare, also mobilizes its military forces covertly. The adversary infiltrates Special Forces to establish connections between various extremist groups, criminal elements and oligarchs in order to conduct synchronized attacks against key infrastructure, communication nodes, organizes riots, sabotage, and occupies governmental buildings. These synchronized actions can take place anywhere in the country in order to distract the attention and resources of the central power, and disable security forces from conducting counterattack on time[247]. If these operations cannot realize the aggressor`s success, it is able to commit its conventional forces to regain initiative and achieve the desired objectives or consolidate gains. Enemy conventional forces also use deterrence by preventing active military countermeasures in Hungary. In order to deter by conventional formations, it is not necessary for the aggressor country to be a neighbor of Hungary, because it can deploy forces to a nearby state under its influence, or could possess sufficient operational reach for military intervention. Furthermore, hostility against Hungary can be only a part of the military operation against the entire NATO, thus the enemy targets the country as a member of the Alliance,

[247] Racz, 63.

not as the main objective. In that case, when the Alliance wages war against another power, Hungary would be involved in the armed conflict despite of her recent diplomatic connection with the enemy.

Economy

As a small state, Hungary has a very vulnerable economy, because it depends on importing raw materials and energy, as well as exporting goods. Hungary was the 35th largest export and the 33rd largest import economy in the world in 2015.[248] By losing top export partners such as Germany or Romania, as well as top import partners like Germany, Austria, China, or even Russia[249] the economy could backslide, and it would result in a decline of the well-being of the population and an increase in the unemployment rate. These issues also reduce the legitimacy of the government. Through immobilizing the flow of energy, the adversary can achieve the same result. Although the economic analysis requires detail beyond the scope of this thesis, changes in economic policy could be an indicator of hybrid attack.

Social

The main battleground for hybrid or unconventional warfare is the society. The adversary can influence it through information, economy and the condition of infrastructure, and the perception of the society affects the legitimacy of the central

[248] AJG Simoes and CA Hidalgo, "The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development" (Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence, 2011), accessed April 6, 2017, http://atlas.media.mit.edu/en/profile/country/hun/.

[249] Ibid.

power and the population`s commitment to patriotism. The occupying power intends to sway citizens to its side, or at least alienate them from the actual government. In order to do so, the opponent can utilize both non-lethal and lethal measures. Non-lethal ones are more preferable, even though they need more time to be effective, but their effect is longer lasting.

In the Ukraine crisis, the presence of a Russian speaking ethnic minority was one of the prerequisites that became the source of legitimacy claim, also the base to influence a part of the population against the central power. In Hungary, the gypsy ethnicity, which constitutes about 7 percent of the total population,[250] can be a source of hostility, not because of their claim for specific territories, but because an adversary can fuel lasting hatred between the gypsy minority and extremist groups. These extremist groups can harass immigrants or foreign citizens, thereby reducing the sense of security of the Hungarian citizenry and discrediting the country. The desire to regain lost land and reunite Hungary and ethnic Hungarians is another rhetoric of far-right parties and extreme groups. Hungary lost two-thirds of its land and one-third of the ethnic Hungarian population after World War I in 1920.[251] The intent to reunite Hungary, or atrocities against Hungarians abroad, could aggravate the connection with neighboring countries or with the international community.

The increasing use of the internet and social media provide more opportunity for the adversary to influence the Hungarian population. The use of the internet itself is a

[250] Sonkoly, 2.

[251] Ibid., 1.

problem for the government, because citizens move away from the central power communication towards individual issues. The decentralization and fractured national identity favor the opponent, which can further separate the citizenry and the central power. Hostile propaganda, false news and hate speech disarrange the individual decision making, thus can underlie the importance of individual versus nation and patriotism.

Information

From the political and military decision makers` perspective, the aggressor tries to achieve fundamental surprise through disinformation, deception, maintaining operational security, timing, disabling intelligence, surveillance and reconnaissance assets, and applying adequate forces and maneuvers. Fundamental surprise is "a challenge for resilience, since by definition it cannot be anticipated, and monitoring is limited by the lack of knowledge about what to target."[252] Russia was able to realize fundamental surprise during the annexation of Crimea, because the hostility was not foreseeable, the Russian intent, objectives, and application of forces were concealed, and not expected. In case an adversary can achieve fundamental surprise during its attack against Hungary, the country would be not prepared for the hostility, would not possess plans for adequate use of forces, policies and resources. Therefore, the opponent could maintain its momentum and freedom of action for a longer period without effective countermeasures from the central power, even realize its own goals without disturbance thereby transitioning to the stability phase.

---

[252] Robert L. Wears and L. Kendall Webb, *Fundamental On Situational Surprise: A Case Study With Implications For Resilience*, Openedition book, 2011, accessed April 4, 2017, http://books.openedition.org/pressesmines/1122?lang=en.

In case the adversary is not able to achieve fundamental surprise, it would attempt to possess at least situational surprise. Events of situational surprise might be temporarily unexpected, but are generally explicable, moreover compatible with the ideas held by the targeted country about the threat.[253] In the Ukraine-Russian conflict, operations against East-Ukraine are under this discretion, when the Ukrainian central power learned from the Crimean case and reacted on time to prevent consolidating gains. From the lesson learned of the Ukraine case, Hungary can identify the commander`s critical information request in order to task intelligence services to monitor tendencies in foreign policy, or any military preparation of a possible adversary. Therefore Hungary, with proper security situational awareness, can detect and prevent fundamental surprise from a hybrid threat, but even in this case we need to assume that the foe would have enough instruments to realize at least situational surprise.

From the view of individual citizens` decision-making, the adversary is able to apply a broad scale of influencing technics to alienate the population from the central power. The most likely instrument of a foe reaching out to the target audience is the internet, because almost 80 percent of Hungarians use it, and more than 50 percent are active on social media. Local radio stations are also potential possibilities for influencing, but they are easier to detect and provide only one-way communication. The Hungarian language is very unique, only the Hungarian ethnic community speaks it; therefore, it is not likely that an adversary transmits an alternative Hungarian language TV channel from abroad; however, it can leverage existing media providers to broadcast hostile messages.

[253] Ibid.

During all phases of a potential hybrid attack, the opponent conducts influence warfare in the cyber domain, human terrain, and via media. By weaponized information, it propagates false news and hate speech to distract Hungarians in order to reduce the support of the central government. The aggressor can also fuel radical movements and parties to attack the constitutional order, the gypsy minority, migrants or other foreigners. By igniting passions in adjacent countries against Hungarian ethnics, e.g. in Romania, Serbia, Ukraine and Slovakia, the adversary can increase the supporting base of radical movements in Hungary that could persecute passing through citizens from these states. These actions reduce the legitimacy of the government, because it cannot protect the Hungarian ethnic group abroad, also discredits the country in the view of the international community. Weaponized information is able to reduce patriotism through narratives, which emphasize that the wellbeing of the individual is more important than fighting for the motherland. The adversary is not limited to these influence measures, but can find or create further vulnerabilities and develop narratives to sway the public opinion.

Synchronized cyber-attacks can also reduce the national power of Hungary, by targeting financial systems, administrative and military objects, communication, different services and power grids. These actions also reduce the legitimacy of the central power, because it cannot defend its citizens and cannot deliver services that the government should provide. Cyber-attacks decrease the command and control capability of security forces as well, thus their ability to counter physical hostile actions. The adversary can take advantage of the relatively cost effective cyber warfare at the commencement of the attack phase in order to disable various defense mechanisms, and cause simultaneous problems for the government and security forces.

The aggressor increases its communication and information superiority in the preparation phase and intends to achieve monopoly at the beginning of the attack phase. In occupied areas, it tries to maintain this superiority in order to gain support for the alternative political power. Through Civil Affairs operations, the foe enables the collaborating government to work effectively, and mitigate causes of instability within civil society. These operations further decrease the support of the legitimate central power, because the occupying forces provide those services, which Hungary cannot. The adversary applies its entire informational power to alienate citizenry from the central power.

Infrastructure

The aggressor intends to secure, destroy or isolate critical infrastructure at the beginning of the attack phase, but also protects those which are necessary for further operations or to enable the collaborative central power. Conducting detailed analysis on infrastructure is beyond the objective of this thesis. However, it must be pointed out that similar to other Western countries, Hungary also has privatized most of its infrastructure that enabled military operations during the Cold War, hence lost its direct control over this capacity. The adversary affects the infrastructure in order to discredit the central power, thus it is not able to provide services, also to paralyze security forces to prevent their operations against occupying forces. Most likely communication installations, bridges, governmental buildings, barracks of security forces, power grids, power plants, hospitals, roads and railways, airports, dams, and major factories are primary objectives to seize, destroy, or protect. By attacking specific infrastructure, the adversary can cause different disasters that not only further decreases the government`s support, but deprive

security forces and resources from the defense sector. The foe can utilize physical actions to impact these objects, like physical destruction and military maneuvers, but also can apply electronic warfare and cyber space operations to realize its goal. Conventional and Special Operational Forces also complement each other's capabilities to make an impact on critical infrastructure, and they can utilize proxies, organized crime groups, as well as bribed officials or individuals, and oligarchs to execute sabotage attacks or occupy key installations.

The invader has great advantage to achieve desired effects against Hungarian critical infrastructure. The aggressor has the initiative, thus can select the time, forces, methods and objectives. It has a broad scale of available forces, like Conventional and Special Forces, proxies, criminals, corrupt individuals, as well as lethal and non-lethal instruments. The HDF`s active duty forces are not able to defend all key infrastructure and simultaneously react to other hybrid operations. However, the opponent has to select its methods wisely to maintain communication to influence the target audience, and to preserve other services and buildings in order to gain support for the new political power.

Physical Environment

The territory of Hungary is 93,028 sq. km,[254] which is relatively small and does not provide large maneuver space for defense in depth. The terrain is overall advantageous for conventional adversary forces` offensive, because it offers almost unlimited maneuver corridors from East and South. Most of the terrain is flat with slight

[254] Central Intelligence Agency, *The World Factbook 2013-14* (Washington, DC: Central Intelligence Agency, 2013).

forestation, which is not preferable for defensive operations, but provides advantage for the opponent. The two main rivers, The Danube, running north to south and The Tisza, running from northeast to southwest, are the main obstacles in the plain region. Large urban areas also can be defensive positions, but an overwhelming enemy could isolate these cities and then advance further. Hills and low mountains, covered by forest, are located in the northern area of the country, and offer restricted and severely restricted terrain for defensive operations, also connection to Slovakia, which is a NATO ally. Hungary`s terrain does not enable effective defensive operations from east and south against a superior conventional force, however it provides restricted and severely restricted terrain that is preferable for defense and connection to a NATO ally to the north.

From the unconventional warfare perspective, the northern hilly and low mountainous area is advantageous for guerilla forces to organize, train and employ troops. Because of the high density of urban areas, continuous forest management, and tourist activity, the adversary needs inaccessible private property to prevent surveillance and detection. Large urban areas are potential terrains for covert underground activities. Because the underground operates in those territories, which are unreachable for guerilla forces, they can take advantage of the population`s density in cities. Sonkoly`s study on extremist groups in Hungary analyzed the hotspots of far-right organizations` activities.[255] Most of these actions were conducted in the vicinity of large urban areas. Although, that did not mean that extremist groups were permanently present in these

[255] Sonkoly, 29.

settlements, but they had the operational reach to support these locations in order to execute operations. Athena institute`s analysis also identified suspected centers of extremist groups, which were located in Budapest, Szeged, Bekes, Bony (in the vicinity of Gyor) and Vac.[256] All of these are cities or town size county capitals. Overall, the terrain is favourable for an adversary to conduct offensive conventional and unconventional operations. NATO membership, in case the conflict crosses the collective defense threshold, enhances Hungary`s operational area, because in this case the fight can extend over the Hungarian border, therefore providing larger maneuver space.

Time

The adversary has the advantage of deciding the time for the commitment of the attack phase, therefore it has the initiative. Most likely the aggressor will determine the time of its preference, when shaping operations in the preparation phase will weaken Hungary`s power enough, and the attack phase can realize the maximum result. In the Ukrainian case, Russia decided the intervention, because the new government intended to align itself with NATO, thus relieving its connection with Russia. In order to prevent this intent, hence losing prestige and power, Russia took advantage of its long preparation activities in Ukraine, as well as its domestic political crisis, to complete the preparation and launch the attack phase. If Ukraine continued a friendly diplomatic approach towards Russia, the annexation of Crimea would not have happened, however Russia would maintain its foreign policy to shape the security environment and wait for another

[256] Athena Istitute, "Gyűlöletcsoport Térkép [Athena Institute-Hate groups map]," Athena Institute, accessed April 7, 2017, http://athenaintezet.hu/gyuloletcsoportok/.

opportunity. In other words, external circumstances also can affect timing, beyond the intent of the aggressor. The lesson learned from the Hungarian perspective is that a collaborative, even friendly power, can become hostile in a short period and depending on its status of preparation can commit the attack phase.

Center of Gravity Analysis

The adversary`s strategic center of gravity in hybrid warfare is the highly integrated central power that allows to synchronize the application of its entire national power. Critical capabilities are military superiority and control over media. Critical requirements are surprise, operational reach of military forces, capability of Special Forces, surrogates, legitimacy of the collaborative government, and denial of involvement in the conflict. Critical vulnerabilities are the perception of the international community, thus possible diplomatic and economic isolation, even NATO intervention, lasting of the conflict and proxy`s support, support of the aggressor`s own population, also the reliability of state sponsored media.

Hungary`s strategic center of gravity is the constitutional order, thus the legitimacy of the central power. Critical capabilities are military deterrence capability, and freedom of the media. Critical requirements are the commitment of the citizenry to patriotism, NATO membership, hence deployable active duty military forces, competent and integrated intelligence, civil preparedness, volunteer reserve forces, and the “whole-of-government” approach. Critical vulnerabilities are impressionable citizens against central power, extremist groups, unconcerned population, grievances between Allies and partners, command and control system, response time and authorities, the legislative system, concrete military capability, and dependency on cyber domain.

Enemy`s Course of Actions

Through the analysis of the Hungarian situation, the author identified the following three potential enemy`s courses of action in the hybrid environment.

Enemy`s most likely course of action: The adversary utilizes all instruments of its national power in order to achieve synergic effect and decentralize Hungarian countermeasures, but fails at realizing fundamental surprise. Full spectrum hybrid operations shape the security environment in the preparatory phase, alienate a portion of the population from the central power, and weaken the legitimacy of the legitimate government. However, the government retains the support of the international community and NATO. The aggressor cannot gain enough proxies to conduct the attack phase exclusively with SOF and surrogates, therefore commits its conventional forces. The involvement of conventional forces exceeds the threshold of Article 5, collective defense agreement, thus NATO can intervene into the conflict. The war takes place in occupied and unoccupied territories.

Enemy`s most dangerous course of action: The aggressor conducts full spectrum hybrid operations, and it is able to procure enough surrogates and supporters to fight against the central power, thus keeping the conflict under Article 5 threshold. With proxies and covert support from SOF and conventional forces, the enemy can achieve fundamental surprise, paralyze the command and control system, successfully fight against Hungarian security forces, and establish functional alternative political power in occupied territories. Hungary has to struggle without official NATO assistance in occupied or unoccupied lands. The adversary introduces the stabilization phase in acquired areas.

Enemy`s limited course of action: The foe does not commit full spectrum hybrid attack against Hungary but goes beyond the limit between white and gray zone. The adversary applies only some instruments of national power, therefore cannot achieve synergetic effect, however can weaken the legitimacy of the government. The aggressor stays under the collective defense limit, thus NATO is not able to support Hungary with military power. The opponent does not intend to overthrow the government or occupy any territory by taking the high risk of possible NATO intervention, but wants to weaken Hungary`s national power, and forces the nation to collaborate with the adversary.

The first part of the analysis identified the threat for which Hungary has to prepare in the hybrid environment. Through the enemy`s courses of actions the author explained how the adversary can apply its hybrid instruments to weaken the country`s power in order to force the nation into collaboration with the aggressor. The following section proposes recommendations for countering the hybrid threat.

Proposed Solution

This part of the analysis answers the second secondary research question: How can Hungary involve its citizenry in order to realize feasible resilience capability? In order to do so, the author follows the steps of Army Design Methodology, hence depicts the desired environment, defines the problem, and recommends an operational approach. Through findings during the process, the thesis underlines those areas where the citizenry`s involvement is necessary to increase Hungary`s resilience capability.

Desired Environment

Hungary is able to maintain its sovereignty and territorial integrity, while sustaining democratic values, and constitutional order. HDF possess expeditionary capability that enables NATO obligations abroad while maintaining its defense capability to protect the country. The majority of the citizenry is committed to repel hostile attack, and has an identified role in the defensive endeavor. The country is protected against fundamental surprise, key infrastructure is identified and secured, critical services are available for HDF and NATO forces during the conflict both in physical and cyber domains. Hostile propaganda cannot impact significantly on the population, thus it possesses the sense of threat, critical thinking, and patriotism. Interagency procedures, authorities, and responsibilities are established and align with legal consideration, as well as other key-stakeholders are identified and involved in the nation`s defense. During armed conflict, in case the deterrence fails, the aggressor in occupied territories is not able to gain support from the population, and activities of the resistance movement are shaping the environment in order to facilitate NATO operations. The Hungarian central power does not accept the aggressor`s gains, but enforces further military opposition.

After the description of the actual and the desired environment, the next step of the Army Design methodology is the identification of the problem.

The Problem

Problem statement: How can Hungary protect its sovereignty and territorial integrity against a great power? Given a small territory that is not favorable for conventional defensive operations, slight active duty and reserve military forces, NATO membership, citizens with a false sense of security, without clearly declared military

threat, widespread internet reliance, developing economy, and dependence on export and import. Facing a superior enemy with centralized national power, military supremacy, utilizing effective influence warfare and Special Operations Forces, and targeting the Hungarian DIME structure simultaneously.

Critical planning factors:

1. Maintain response capability for NATO collective defense obligation in support of other Allies.
2. The solution must consist of NATO civil preparedness ability in order to support HDF and NATO operations in the country.
3. Reintroducing the conscription is not acceptable option according to the ruling government.
4. Despite increasing the military budget, the proposed solution must be economical, due to the condition that financial expenses have to cover the modernization of the active duty forces as well.
5. Because Hungary has no declared enemy, therefore no clearly identified threat, the solution has to contain various methods to reach out to the citizenry and unite it under patriotism.
6. Because the threat is hybrid in nature, the proposed concept also has to counter perils on all possible domains, against conventional and unconventional methods, also in the enemy`s unoccupied and occupied territories.

7. The plan has to facilitate interagency effort and involve key governmental and private stakeholders in order to enhance cooperation among the nation`s DIME powers.
8. The solution cannot overwhelm active duty forces, due to their commitment in other tasks, such as deployments and NATO collective defense obligation.
9. Legislation must support the timely and integrated response against hybrid attack with clear decision-making authorities.

Operational Approach

The proposed solution against hybrid warfare must answer the most likely and most dangerous enemy`s courses of action at once. If it does so, the solution will cover the enemy`s limited courses of action as well.

The operational approach consists of seven conditions and eight lines of effort in order to achieve the desired end-state. The diagram aligns instruments of national power to each line of effort. There are 24 identified tasks dispersed among relevant lines of effort. Tasks belong to multiple efforts, while some appear in different phases of hybrid war. Seven lines of effort support the “Gain commitment of citizenry for the nation`s defense” line of effort. The diagram shows that in the preparatory phase, the involvement of people increases moderately, while in the attack phase it grows at a higher rate, but in the last phase, declines drastically. The following paragraphs provide further explanation of figure 1.

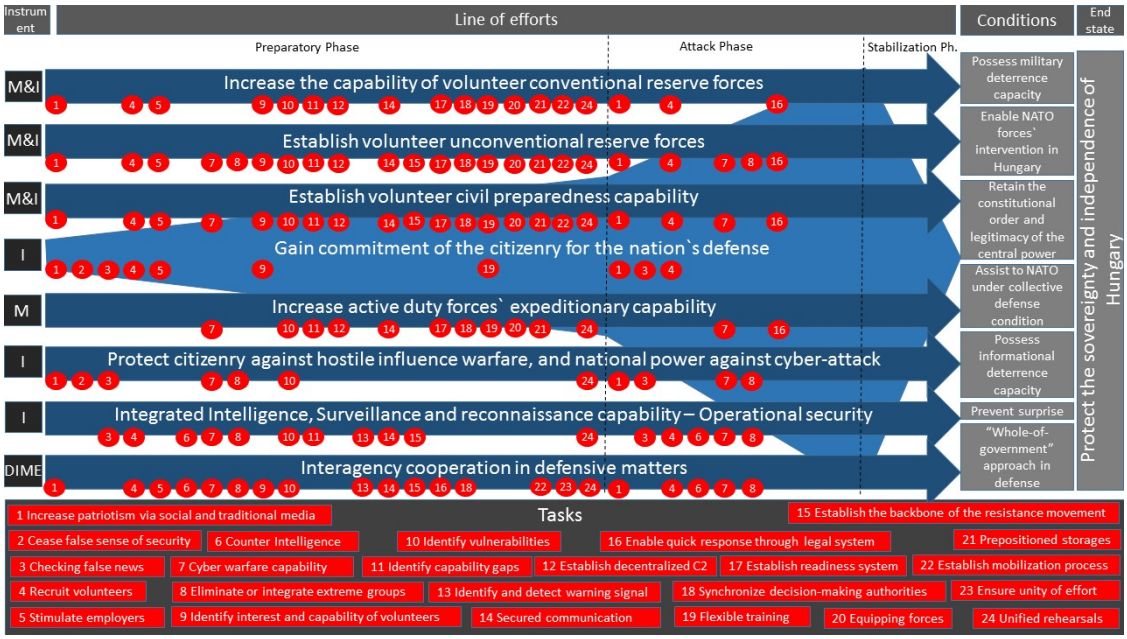

Figure 1. Operational Approach

Source: Created by author.

Risks and Mitigation Measures

The proposed solution contains several risk factors, therefore the following section analyses the most important risks and offers mitigation measures. The primary risk of the proposed solution is whether the country can reach out and influence a sufficient number of volunteers. The involvement of a large segment of the population in defense sector increases the vulnerability of operational security, causes command and control challenges; requires further financial, manpower, and material resources, as well as time. Furthermore, volunteer unconventional reserve forces that have the capability to conduct resistance against an occupying power, also have the capability to overthrow the existing government through insurgency.

In order to gain an adequate number of volunteers for the nation`s defense, the central power has to initiate an influence campaign, the military has to offer appropriate tasks for each individual and employers also have to enable the endeavor. The Information instrument of national power can establish an environment where patriotism is a preferable value for the society. The narrative must emphasize the possible threat against Hungary, as well as the importance of NATO membership and the obligations that go along with it.

Volunteer defense forces request different capabilities for different tasks. Conventional territorial defense formations need diverse physical and mental abilities than members of cyber warfare, civil preparedness, guerilla forces or auxiliary units. The Military instrument of national power has to align on individual capability and desire to positions in resilience. Each volunteer`s proficiency and determination for patriotism are more crucial than his or her shortfalls. This flexibility can recommend more members for Hungary`s resilience capacity, but request a more complex structure, training and command and control system.

Employers have to be involved in the resilience and they must be assured that they would not suffer disadvantages because their employees volunteered for reserve forces. In other words, volunteers must keep up their jobs while they are serving in reserve positions. Therefore, the military has to offer flexible training events in time and location that align with volunteers` jobs. The central power also can offer benefits for employers to encourage retainers` involvement in national defense. Furthermore, the government has to compensate the time and effort of reserve forces` members.

Augmented reserve military forces can be more vulnerable against espionage. In order to mitigate that risk, HDF have to employ operational security measures to protect communication means between command elements and service members and have to align security status to volunteer positions. Some of these assignments do not need security classification, like most of civil preparedness positions or conventional reserve forces members; those who work in cyber security areas or belong to the underground pose a higher security risk.

Larger volunteer military forces require a different command and control structure, especially the resistance movement due to its highly decentralized nature. Emphasizing decentralization and mission command philosophy through disciplined initiative reduces the size of command element in higher headquarters not only in unconventional formations, but also in territorial defense units or in the civil preparedness. If trained and educated volunteers can fill up most of the command positions that could decrease the burden of active duty service members. Delegated decision-making is crucial in a hybrid environment, because the aggressor effects simultaneously in time and space, hence making centralized control impossible.

A larger military structure requires more resources, however the needs of unconventional forces and civil preparedness is lower than conventional formations. Territorial defense units with modern anti-tank and anti-aircraft weapon systems, and communication equipment are more expensive, than guerilla forces, the underground or even civilians who provide services for combat units. Time is another vital resource to consider, because the establishment of a complex volunteer reserve force with diverse

capabilities is a lasting effort, and the enemy has a vote about how much time it allows to Hungary for the preparation.

Because UW applies the same capability to establishing resistance movement against an occupying power, as for insurgency to overthrow the legitimate government, Hungary has to be sure that she maintains control over unconventional forces. In order to mitigate this risk, the military has to emphasize the importance of patriotism and independence from political parties during training events, also must supervise adversary`s or radical groups` influence on reserve forces. The next section highlights those areas where citizenry can participate in resilience, thus responds to the second secondary research question.

Involvement of Citizenry

In order to protect the country`s center of gravity, the constitutional order, hence the legitimacy of central power, Hungary has to strengthen its primary critical requirement, the committed citizenry for the nation`s defense. The state needs to maintain popular support for democratic values and central power, while simultaneously influencing the citizenry to take part in resilience, hence defensive activities. According to the analysis so far, the Military segment of national power requires civilian augmentation, therefore volunteers in three different areas. First, in conventional volunteer reserve forces, which intends to organize on territorial bases. Second, in unconventional volunteer reserve forces, as resistance movement, which extend the capability of conventional warfare, due to its operational reach to occupied territories. Third, in civil preparedness, where volunteers enable conventional forces operations in

unoccupied territories, and support UW operations as auxiliaries in enemy controlled areas.

The capability of territorial defence units can facilitate the protection of key infrastructure, anti-diversion, and traditional defensive operations. Volunteers for these conventional formations need adequate physical condition and proficiency in basic infantry, artillery, anti-tank, and air defense weapon systems. They can be equipped as light or mechanized infantry; however, both specialties need combat service support augmentation. Members of these units can also replace positions in active duty forces, if there are shortages or suffered attrition in combat. Realizing an offense capable territorial organization, such as Russia intends to do, takes time and significant resources.

Resistance movement provides a different capability for the HDF, also request diverse abilities from volunteers and less expensive equipment. Guerillas can operate in restricted and severely restricted terrains, harassing the adversary in its security areas. While the underground is able to operate in urban terrain by taking advantage of high-density population. Although both guerillas and underground volunteers need similar physical conditions, and organization on territorial bases, they require less sophisticated weapon systems than conventional forces. Auxiliaries enable the resistance movement with logistic support, safe havens, and information, but they are not involved in combat, thus they do not need strong physical condition.

The civil preparedness has the greatest opportunity to involve a large segment of citizenry and take advantage of the civilians` professionalism. These experts can provide basic services, such as energy, transport, food, water, medical support, and communication for the military and civil population. Furthermore, they can take part in

cyber operations, civil defence, identifying key vulnerabilities, checking hostile propaganda, reporting adversary`s influences in private sector or in radical movements, advising information operations, and educating the younger generation in patriotism and social values. These volunteers do not need special physical condition to fulfil these objectives, but the effect of their effort could be very significant. They also can provide support for the resistance movement in occupied territories by augmenting auxiliaries. Furthermore, these civilians are able to organize and participate in non-violent resistance.

The aforementioned three segments of resilience, the territorial conventional volunteer forces, resistance movement, and civil preparedness, provide diverse capabilities for Hungary to protect its sovereignty. However, this diversity is also important for volunteers, because they can select from different opportunities, and they can participate in the national defense, despite their physical condition, mental capacity, age, gender, business, agenda or skill. The following section answers the primary research question through the mission narrative.

Mission Narrative

Hungary needs a hybrid approach in her defense strategy to militate against potential hybrid threats. The Military instrument of the national power has to extend its mainly lethal effect and must facilitate the Information power to protect Hungary`s sovereignty through the involvement of citizenry. In order to facilitate the nation`s interest, the HDF has to retain the constitutional order and the legitimacy of the central power, procure military deterrence capacity, prevent the aggressor`s fundamental surprise, enable NATO operations in the country, and assist allies under collective defense conditions. Simultaneously they need to support other agencies establishing an

informational deterrence capability to protect the population against hostile propaganda and cyber-attack. Because of the nature of hybrid warfare, the Military instrument is highly dependent on other instruments of the national power, thus the HDF must maintain collaboration with other stakeholders to establish and preserve a “whole-of-government” approach.

In order to realize desired conditions, the analysis has identified eight lines of effort. The only exclusively Military line of effort is the active duty forces` expeditionary capability, which intends to enable NATO collective defense obligations, while maintaining capability for homeland defense as well. To enable the Informational instrument, the HDF needs to collaborate with other agencies and stakeholders to conduct the following lines of effort: gain the citizenry`s commitment to the nation`s defense, protect the population against hostile propaganda and cyber-attack, as well as integrated ISR and operational security. Three lines of effort require close cooperation between the Military and Informational instruments, which directly involve the citizenry in the resilience effort: increasing the capability of conventional territorial reserve force, establishment of volunteer unconventional reserve forces or in other words resistance movement, and the creation of civil preparedness capacity. Interagency cooperation is the final line of effort that facilitates the connection to other instruments of the national power in order to achieve unity of effort among various stakeholders.

The success of Hungary in the hybrid environment depends on the achievements in the preparatory phase. Through the citizenry`s patriotic commitment, thus the united will of the people to protect the motherland, with the three different types of volunteer organizations and integrated information operations, the country can introduce a massive

deterrence capability. This capability has much more significance than merely the active component of HDF combined with volunteer territorial defense forces. This is not only because of their higher numbers, but their ability to fight in occupied areas by maintaining the willingness of the isolated population to resist, involve extensive proficiency from private sector, establish unity of effort among instruments of the national power, and minimize the disadvantage of the terrain. If the deterrence fails, the country still has the capability to realize success in the attack phase; however, this success also depends on the fulfilment in the preparatory phase.

The adversary intends to shorten the period of armed conflict in the attack phase, therefore each deficiency in the preparation could cause defeat for the country, such as resignation from independence or territory. If the resistance movement or civil preparedness does not function before the aggression, it is not likely that Hungary can establish these capabilities during the attack phase and support conventional operations effectively. However, increasing the capacity of these volunteer organizations is still possible during active combat operations, if their backbone already exists and is operating.

In the temporary security environment, Hungary cannot allow that her military strategy depends only on traditional means. Resilience, flexibility, and adaptability have to be the traits of the defense sector to counter hybrid threats. In order to achieve deterrence capability, Hungary, as a small country, has to involve citizenry that possesses the proficiency and the manpower against the aggressor. However, the state must use its Informational instrument to influence these people to strengthen the Military instrument

of the national power. The military has to find the proper position for each individual according to his or her advantages and intention, but not by their shortcomings.

Summary and Conclusions

The analysis applied the Army Design Methodology in order to respond to the primary and secondary research questions, through the introduction of the threat, the proposed solution, and the mission narrative. Chapter 5 discusses the result of the analysis, its possible applications, and underlines unexpected findings. The following chapter also provides recommendations for further studies in this topic and proposes actions for decision-makers.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Introduction

The purpose of this study is to generate options for the HDF decision makers regarding the Military and Informational instruments of national power in order to strengthen Hungary's resilience against hybrid warfare.

This last chapter briefly summarizes the findings from the analysis, interprets the result, draws up implications, and highlights unexpected findings. As well as it offers recommendations for further studies and possible actions that facilitate the Hungarian resilience against hybrid threats. Finally, the author synthesizes chapter 5 and formulates a conclusion.

Chapter 4 examined the threat that a hostile great power can inflict against Hungary. The adversary uses the vantages of hybrid warfare in order to take advantage of its superiority in the entire DIME structure of the national power over the small state, cause surprise, and generate simultaneous provocation for Hungary. The aggressor targets the legitimacy of the Hungarian government through discord and division in the citizenry. The foe intends to achieve its goals without or with only very limited open armed conflict to avoid NATO intervention.

Hungary, in order to prepare the country for hybrid attack, has to establish resilience, which provides flexible and adaptive countermeasures against a powerful enemy. The resilience has to consist of traditional military capability, but also has to possess non-traditional methods such as resistance movement and civil preparedness. Through these methods, the country can involve other governmental agencies, private

sector, civilian experts, and more importantly the citizenry`s will to fight for national sovereignty. Hybrid threat necessitates hybrid approach in the defense strategy, which provides the crucial flexibility and adaptivity against conventional and unconventional warfare, as well as offenses on all possible domains against every instrument of the state`s DIME power. However, this endeavor highly depends on the patriotic commitment of the Hungarian citizenry. The interaction between Military and Informational instruments can offer areas where the population can participate in the nation`s defense. Volunteer territorial defense forces with conventional capability, resistance movement with unconventional capability, also the civil preparedness that enables military operations and provides freedom of action are the main elements of the nation`s resilience. Other lines of effort also support resilience, such as active forces` expeditionary capability, intelligence, patriotic commitment, protection against hostile propaganda, and interagency cooperation.

Following the summary of findings in chapter 4, the next section offers additional interpretations.

Interpretation of Results

This part of the Conclusion and Recommendations chapter explains findings from the analysis, provides further implications and collects unexpected findings. In other words, this section describes the importance of outcomes from chapter 4.

Explanation of Findings

A small state can generate significant military capacity through the involvement of citizenry, while decreasing its vulnerability against hostile influence warfare. The

capability of volunteer organizations has to promote conventional abilities support of military operations in unoccupied territories, unconventional abilities enable effects in the enemy`s security areas or occupied territories, and combat service support abilities create conditions for combat units.

By providing further capabilities for the HDF, different volunteer organizations also provide options for volunteers to join the resilience with diverse abilities. Furthermore, applying multiple opportunities for the resilience endeavor could increase cost effectiveness. In other words, the same expense on defense sector offers greater number of participants than spending the same amount on completely conventional reserve forces. More participants mean more defense capacity and more citizens who are dedicated to patriotism. The next paragraphs describe further implications.

Implications

The threat, thus the common enemy, is a very important motivation for citizens to join volunteer organizations. In Lithuania, the threat was not enough to attract adequate quantity of volunteers for TDF, hence the state has had to reintroduce conscription. In Hungary, where the threat is much lower than in Lithuania, the Informational instrument has to develop methods to attract the population, while the Military instrument has to offer seductive possibilities to engage citizens. If there is no defined threat, people are minded to select their own, an object to hate and fight against. Ethnic minorities such as gypsies, immigrants, and foreigners are typical targets for hate groups. Through a designated common enemy, the central power could leverage these radical groups and other segments of the population to concentrate their extra vigor against the aggressor of the nation.

The mobilization and readiness of volunteer organizations are a very crucial part of establishing a new military strategy. Because the surprise and the momentum are vital for the aggressor, the response time of Hungarian forces is critical as well. Therefore, HDF and its volunteer formations need a command and control system that assigns missions to subordinate headquarters quickly while maintaining secured and accessible communication with each member. Further requirements for these communication systems are resistance against cyber-attacks and electronic warfare operations, support multiple ways, and cost effectiveness. Islamic State and other terrorist organizations use applications on cyber domain for control and communication,[257] thus Hungary should examine the feasibility of this option as well. Hungary has to reward those volunteers who undertake higher readiness standards. Each individual has different circumstances, e.g. job and family commitment; therefore, the compensation has to differ among different readiness obligations.

It is important to declare that soldiers of TDF with conventional training, equipment, and sustainment cannot become guerilla or underground fighters overnight, when the enemy occupies their territory. Regular and irregular soldiers require different capabilities; furthermore, acquiring sufficient capabilities takes significant time. Volunteers cannot be dual hatted with regular and irregular tasks, because both professions would suffer shortage.

[257] Sebastian Rotella, "The Dark Side of Privacy: How ISIS Communications Go Undetected," Pacific Standard, July 29, 2016, accessed April 22, 2017, https://psmag.com/the-dark-side-of-privacy-how-isis-communications-go-undetected-890aec4e86c3.

Unexpected Findings

Before detailed research, the thesis intended to concentrate exclusively on irregular augmentation to active duty forces. By the examination of NATO documents and individual countries` defense strategy, the focus extended to TDF and civil preparedness possibilities as well. Through researches and analysis, it became clear that these extra capacities could augment and complement each other by expanding maneuver space, number of involved citizens, and realizable objectives.

The potential of non-violent resistance was another finding that could significantly increase the effectiveness of resistance movement in occupied territories. However, it also requires planning, preparation, and organizing procedures; its achievement could realize great success in influencing warfare.

The adaptive and reassuring legal environment is one of the most crucial elements in countering hybrid warfare. The aggressor easily can take advantage of shortages in legislation, which does not enable quick decision-making and unity of effort, possess unclear authorities and rules of engagement for the Hungarian security forces. In hybrid environment every hour and every minute counts, thus the responsible commander must know the political intent, command relationship, available resources, and adaptable measures immediately. The next part accumulates recommendations for additional research and study, as well as proposes necessary actions.

Recommendations

This thesis is not able to examine all aspects of the Hungarian resilience, due to time limitation and required comprehensive competency in various areas. Through Army Design Methodology, this work only develops a solution by utilizing conceptual

planning, but adjustments from subject matter experts and detailed planning process are inevitable. Therefore, the following paragraphs highlight those issues, which require detailed analysis in order to facilitate adequate decision-making.

Proposals for Further Study

HDF has to determine missions, capabilities, and desired effects of TDF, resistance movement, and civil preparedness. Planners also have to identify these organizations` structures, specified positions, requirements, and security status where civilians can participate. Decision-makers need cost estimation of establishment, sustainment, and equipping these volunteer formations. The central power has to devise an elaborate incentive system that rewards members` participation, effort, usefulness, as well as readiness and mobilization conditions in the nation`s defense.

Because countering hybrid warfare necessitates interagency, as well as intergovernmental effort, while involving stakeholders in NGOs and the private sector, realizing unity of effort is very challenging. Hungary has to work out a command and control system that integrates these key-stakeholders, clarifies authorities, establishes supported and supporting relationships, and adjusts the system to legal considerations.

The cyber domain offers a unique capability to reach out and influence citizenry, even for secured communication, as different terrorist organizations utilize it. Therefore, Hungary needs to examine this capability in order to maintain a cost effective informational means with a large segment of the population.

Training and education are crucial segments of volunteer organizations. Through training, participants must acquire knowledge to fulfill their positions, handle weapon systems, become leaders etc. Parallel to training, they have to receive education about

patriotism, critical thinking, and social values to protect them from hostile influence warfare. Therefore, planners have to develop training and education structure for TDF, resistance movement, and civil preparedness members and units. In order to elaborate training and education programs, developers must consider time and cost effectiveness, hence they need to apply distance learning through internet where appropriate, as well as training events where the physical presence is indispensable. Commitment approach versus compliance is also crucial in training; therefore, the system has to reward volunteers who undertake more, but also has to enable those who are not able to participate as much.

After summing-up recommendations for further studies, the following section offers necessary actions to facilitate Hungary`s resilience capacity.

Recommendations for Action

Hungary has to measure performance and effectiveness of the endeavor against hybrid threats. The state can estimate the performance through the number of volunteers, how much time and effort they spend for defense related tasks. Polls, joint or unified exercises, and response to natural disasters or limited hybrid-attacks can be indicators of effectiveness. Through polls, the central power can measure the citizens` interest in patriotism, their potential will to fight, population`s sense of security, and how to involve more volunteers. Results from polls enable adjustments in the system to revise the efficiency of recruitment, influence operations, training, command structure, and readiness.

The Hungarian central power, in collaboration with experts from the private sector, needs to devise an influencing strategy, in order to reach out to citizenry and

involve them in resilience endeavor. Without this strategy, it is not likely that citizens will understand the threat in the recent security environment and participate in defensive efforts. Thus, the nation needs a well-structured narrative that emphasizes and names potential threats, as well as highlights social values such as the importance of the nation-state, protection of homeland, constitutional order, individual`s role and responsibility in the nation`s defense, and the meaning of being in an alliance.

Because the preparation phase of hybrid warfare is already ongoing in Hungary, the nation has to actuate countermeasures against it immediately. TDF, resistance movement, and civil preparedness request significant time to become effective, hence the country must start preparation as soon as possible.

Finally, the last section provides summary on chapter 5 as well as addresses the conclusion.

Summary and Conclusions

The last chapter has synthesized findings during the analysis process as well as has recommended areas for further studies as well as for actions. As this thesis is a one-man effort, yet conceptual planning requires versatile skills, therefore this proposed solution cannot be complete and detailed enough. Is it unquestionable that the citizenry possesses a great potential, which is crucial to defend a small country such as Hungary. However, the nation must gain the support and commitment of its population in order to establish resilience against various threats of hybrid warfare. The Military and Informational instrument of the national power have capabilities to do so.

This thesis started with Clausewitz`s words about the relationship between policy and military operations. His statement holds only partially true in Hungary`s

contemporary security environment. Central power is definitely interested in the resilience through its potential values, requirements, and utilization. However, the central power also has to consider and understand the resistance`s value to the people in order to involve citizenry for the nation`s defense before it is too late, because the enemy has already leveraged them and has started the hybrid offensive.

BIBLIOGRAPHY

Athena Istitute. “Gyűlöletcsoport Térkép [Athena Institute–Hate Groups Map].” Athena Institute. Accessed April 7, 2017. http://athenaintezet.hu/gyuloletcsoportok/.

Barabas, Janos T. *Information Warfare in Hungary*. Policy Brief. Budapest: Institute for Foreign Affairs and Trade, 2017.

Bartkowski, Maciej. “Countering Hybrid War: Civil Resistance as a National Defence Strategy.” Open democracy, May 12, 2015. Accessed March 23, 2017. https://www.opendemocracy.net/civilresistance/maciej-bartkowski/countering-hybrid-war-civil-resistance-as-national-defence-strateg.

Bragg, Belinda. “Specifying and Systematizing How We Think about the Gray Zone.” NSI Team, July 27, 2016. Accessed January 5, 2017. http://nsiteam.com/social/wp-content/uploads/2016/12/CP-1-Definition-of-Gray-06-27-2016-Final.pdf.

Cederberg, Aapo, and Pasi Eronen. “How Can Societies Be Defended against Hybrid Threats.” Fortuna`s corner, November 6, 2015. Accessed November 12, 2016. http://fortunascorner.com/2015/11/06/how-can-societies-be-defended-against-hybrid-threats/.

Central Intelligence Agency. *The World Factbook 2013-14.* Washington, DC: Central Intelligence Agency, 2013.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Efthymiopoulos, Marios P. “NATO Smart Defense and Cyber Resilience.” Fletcher, May 2016. Accessed January 31, 2017. http://fletcher.tufts.edu/~/media/Fletcher/Microsites/Karamanlis%20Chair/PDFs/Karamanlis_WP_May_2016.pdf.

Gomez, Ayana. “Human Networking.” September 11, 2015. Accessed January 29, 2017. https://prezi.com/j-hh_9kpe5ag/human-networking/.

Headquarters, Department of the Army. Field Manual (FM) 3-05.130, *Army Special Operations Forces Unconventional Warfare.* Washington, DC: Headquarters, Department of the Army, 2008.

———. Army Techniques Publication (ATP) 5-0.1, *Army Design Methodology.* Washington, DC: Headquarters, Department of the Army, 2015.

———. Training Circular (TC) 18-01, *Special Forces Unconventional Warfare.* Washington, DC: Headquarters, Department of the Army, 2010.

———. Army Doctrine Publication (ADP) 3-05, *Special Operations.* Washington, D.C: Headquarters, Department of the Army, 2012.

———. Field Manual (FM) 5-0, *The Operations Process.* Washington, DC: Headquarters, Department of the Army, 2010.

Hungarian Central Statistical Office, KSH. "The Proportion of Internet Users within the Population." Accessed March 29, 2017. http://www.ksh.hu/docs/eng/xstadat/xstadat_annual/i_oni016.html.

Hungarian Ministry of Defence. "Relations Must Be Strengthened between the Hungarian Defense Forces and Society." Website of the Hungarian Government, November 25, 2016. Accessed January 17, 2017. http://www.kormany.hu/en/ministry-of-defence/news/relations-must-be-strengthened-between-the-hungarian-defence-forces-and-society.

———. "Hungarian Defence Forces." Honvedelem.hu. Accessed January 17, 2017. http://www.honvedelem.hu/files/9/5294/imazs-angol.pdf.

———. "Hungary`s National Defence Strategy." Website of the Hungarian Government, 2012. Accessed March 28, 2017. http://2010-2014.kormany.hu/download/b/ae/e0000/national_military_strategy.pdf#!DocumentBrowse.

INFOSEC Institute. "Cyber Warfare and Cyber Weapons, a Real Growing Threat." INFOSEC Institute, January 15, 2015. Accessed March 16, 2017. http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/#gref.

Joint Chief of Staff. Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States.* Washington, DC: Joint Chief of Staff, 2013.

———. Joint Publication (JP) 3-05, *Special Operations.* Washington, DC: Joint Chief of Staff, 2011.

Kofman, Michael. "Russia's Territorial Defense Battalions Are Finally Here." Russian Military Analysis, September 2, 2016. Accessed March 21, 2017. https://russianmilitaryanalysis.wordpress.com/2016/09/02/russias-territorial-defense-battalions-are-finally-here-all-two-of-them/.

Kaska, Kadri, Anna-Maria Osula, and LTC Jan Stinissen. "The Cyber Defence Unit of the Estonian Defence League." 2013. Accessed February 20, 2017. https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf.

Lalor, John Joseph. *Cyclopædia of Political Science, Political Economy, and of the Political History of the United States.* Chicago, IL: Melbert B. Cary & Company, 1884.

Lucas, Edward, and Ben Nimmo. “Information Warfare: What Is It and How to Win It?” CEPA, November 2015. Accessed February 12, 2017. http://cepa.org/sites/default/files/Infowar%20Report.pdf.

Maigre, Merle. “Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO.” The German Marshall Fund of the United State, February 12, 2015. Accessed February 12, 2017. http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato.

Marton, Peter, and Peter Wagner. “The Impact of Hungary`s NATO Membership. Intra-Allience Adaptation between Soft Constrains and Soft Subversion.” In *Newcomers No More? Contemporary NATO and the Future of the Enlargement from the Perspective of ‘Post-Cold War’ Memebers*, edited by Robert Czulda, and Marek Madej, 137-152. Warsaw, Prague, Brussels: International Relation Research Institute in Warsaw, NATO Information Center in Prague, 2015.

Military Factory. “Military Terms.” Military Factory. Accessed December 11, 2016. http://www.militaryfactory.com/dictionary/military-terms-defined.asp?term_id=4584.

Monaghan, Andrew. “Putin’s Way of War.” *Parameters* 45, no. 4 (Winter 2015-16): 65-74. Accessed November 20, 2016. http://strategicstudiesinstitute.army.mil/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf.

Morgenthau, Hans. *Politics among Nations: the Struggle for Power and Peace.* New York: McGraw-Hill, 1993.

Morris, Victor R. “Grading Gerasimov-Evaluating Russian Nonlinear War through Modern Chinese Doctrine.” *Small Wars Journal,* September 17, 2015. Accessed January 2, 2017. http://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine.

MTI. “The Hungarian Defence Forces Must Be Made a Major Military Force in the Region by 2026.” Website of The Hungarian Government, February 16, 2017. Accessed March 24, 2017. http://www.kormany.hu/en/ministry-of-defence/news/the-hungarian-defence-forces-must-be-made-a-major-military-force-in-the-region-by-2026.

NATO. “NATO Summit Guide Warsaw 2016.” NATO Public Diplomacy Division, July 8-9, 2016. Accessed January 11, 2017. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf.

———. “Wales Summit Declaration.” September 5, 2014. Accessed January 30, 2017. http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO ACT. “Strategic Foresight Analysis 2015 Update Report.” 2015. Accessed January 27, 2017. http://www.act.nato.int/images/stories/media/doclibrary/160121sfa.pdf

NATO Cooperative Cyber Defence of Excellence. “Cyber Definitions.” Accessed January 16, 2017. https://ccdcoe.org/cyber-definitions.html.

Newson, Robert A. “Why US Needs Strategy to Counter Hybridwarfare.” *Defense One*, October 23, 2014. Accessed Januar 14, 2017. http://www.defenseone.com/ideas/2014/10/why-us-needs-strategy-counter-hybridwarfare/97259/.

Nikers, Olevs. “Inside Latvia’s New Defence Strategy-Riga Declares Its Military Ambitions.” LRT, June 7, 2016. Accessed March 21, 2017. http://www.lrt.lt/en/news_in_english/29/139072/inside_latvia_s_new_defence_strategy_riga_declares_its_military_ambitions.

Orban, Viktor, The Prime Minister of Hungary. Inteview with Viktor Orban, interview by Katolikus Radio, Budapest, Hungary, October 29, 2016.

Parliament of Hungary. “35/2016. (XII. 19.) OGY határozat.” *Magyar Közlöny* no.208 (December 19, 2016): 82616-82790.

Praks, Henrik. *Hybrid or Not: Deterring and Defeating Russia`s Ways of Warfare in the Baltics-the Case of Estonia.* Rome, Italy: NATO Research Division, 2015.

Racz, Andras. “Russia’s Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist.” FIIA Report, Helsinki, Finland: The Finnish Institute of International Affairs, 2015.

Reed, Tristan. “Intelligence and Human Networks.” *Stratfor*, January 10, 2013. Accessed March 11, 2017. https://www.stratfor.com/weekly/intelligence-and-human-networks.

Riigi Teataja. “The Estonian Defence League Act.” February 28, 2013. Accessed December 2, 2016. https://www.riigiteataja.ee/en/eli/525112013006/consolide.

Rotella, Sebastian. “The Dark Side of Privacy: How ISIS Communications Go Undetected.” Pacific Standard, July 29, 2016. Accessed April 22, 2017. https://psmag.com/the-dark-side-of-privacy-how-isis-communications-go-undetected-890aec4e86c3.

Simoes, AJG, and CA Hidalgo. “The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development.” Workshops at the Twenty-Fifth AAAI Conference on Artificial Intelligence, 2011. Accessed April 6, 2017. http://atlas.media.mit.edu/en/profile/country/hun/.

Singer, P. W. “How Can America Beat Russia in Cyber War, Despite Trump.” Wired, January 14, 2017. Accessed January 30, 2017. https://www.wired.com/2017/01/america-can-beat-russia-cyber-war-despite-trump/.

Sonkoly, Tibor K. “Aggressive Neighborhood Watch or Unconventional Threat? The Hungarian Extreme Right-Wing Self-Defense Movements.” Master`s Thesis. Naval Postgraduate School, Monterey, CA, 2014.

Spencer, Jack. “The Facts about Military Readiness.” Heritage, September 15, 2000. Accessed November 20, 2016. http://www.heritage.org/research/reports/2000/09/bg1394-the-facts-about-military-readiness.

Stake, Robert E. *The Art of Case Study Research.* Thousand Oaks, CA: SAGE Publication, 1995.

Statista. “Forecast of Social Network User Numbers in Hungary from 2014 to 2021.” Statista, Accessed March 29, 2017. https://www.statista.com/statistics/568952/predicted-number-of-social-network-users-in-hungary/.

Szymanski, Piotr. “The Baltic States’ Territorial Defence Forces in the Face of Hybrid Threats.” OSW, March 20, 2015. Accessed March 21, 2017. https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-03-20/baltic-states-territorial-defence-forces-face-hybrid-threats.

The Baltic Times. “Lithuania to Reintroduce Permanent Conscription.” *The Baltic Times*, March 15, 2016. Accessed April 18, 2017. http://www.baltictimes.com/lithuania_to_reintroduce_permanent_conscription/.

The National Academy of Defence of the Republic of Latvia. “Resistance Seminar Series.” After Action Report, Riga, Latvia: The National Academy of Defence of the Republic of Latvia, 2015.

Toor, Amar. “Facebook Rolls Out Fake News Filter in Germany.” The Verge, January 15, 2017. Accessed January 30, 2017. http://www.theverge.com/2017/1/15/14277964/facebook-fake-news-filter-germany.

Tucker, Patrick. “The US Is Losing at Influence Warfare. Here’s Why.” *Defense One*, December 5, 2016. Accessed February 12, 2017. http://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/

Wears, Robert L., and L. Kendall Webb. *Fundamental On Situational Surprise: A Case Study With Implications For Resilience*. Openedition books, 2011. Accessed April 4, 2017. http://books.openedition.org/pressesmines/1122?lang=en.